HELSINKI SCHOOL OF ECONOMICS (HSE)

Department of Accounting and Finance

EFFECT OF THE SARBANES-OXLEY ACT OF 2002 S404 ON INTERNAL CONTROL PRACTICE

HELSINGIN
KAUPPAKORKEAKOULUN
KIRJASTO

9834

Accounting

Master´s thesis

Reetta Liikala

Fall 2005

Approved by the Council of the Department 6 / 9 2005 and awarded the grade excellent 80 points

KTT Pontus Troberg KTT Lasse Niemi

HELSINKI SCHOOL OF ECONOMICS (HSE)
Master's Thesis
Reetta Liikala

ABSTRACT
August 29, 2005

EFFECT OF THE SARBANES-OXLEY ACT OF 2002 S404 ON INTERNAL CONTROL PRACTICE

Purpose of the Study

The objective of this thesis is to depict the effect of the Sarbanes-Oxley Act of 2002, S404 on internal control practice. The study aims to describe the effects that the act has on a company's internal control system. The research problem is explicitly examined from a management's point of view.

The study examines the concept of internal control, the essential recommendations on internal control prior to the Sarbanes-Oxley Act S404, and the requirements of Section 404. The empirical study researches internal control practice in one case company and examines the changes that the S404 has brought to the case company's internal control system.

Methodology and Data

The research method of this thesis is a case study and one case company is examined. Research material includes questionnaires, interviews, direct observation, archived records and documentations.

Results

Results indicate that the definition of internal control is still quite vague. There is a trend from a narrow scope toward a broader scope definition. Internal control is considered to be a part of a company's corporate governance. The Sarbanes-Oxley Act S404 is the first initiative that forces companies' management to assess internal control over financial reporting.

The research results drawn from the in-depth case analysis are as follows: (1) management's positive attitude toward internal control is a key factor in an effective internal control system, (2) the purpose of internal controls should be effectively communicated to all employees, (3) S404 has increased the number of controls (4) S404 has led to a more risk-oriented way of thinking and a more process-oriented mind.

This thesis presents recommendations for the case company that are divided into three classes. The first class covers factors that enable an effective internal control system and the second class involves recommended changes to current internal control processes. The third class includes information and communication related recommendations.

Keywords
Internal Control, the S404 of the Sarbanes-Oxley, the COSO Framework

HELSINGIN KAUPPAKORKEAKOULU
Laskentatoimen tutkielma
Reetta Liikala

TIIVISTELMÄ
29.08.2005

SARBANES-OXLEY 2002 –LAIN KOHDAN 404 VAIKUTUS SISÄISEN VALVONNAN KÄYTÄNTÖÖN

Tutkimuksen tavoitteet

Tutkimuksen tarkoituksena on kuvailla Sarbanes-Oxley 2002 –lain kohdan 404 vaikutusta sisäisen valvonnan käytäntöön. Tutkimuksen tavoitteena on kuvata vaikutuksia, joita lailla on yrityksen sisäiseen valvontajärjestelmään. Tutkimusongelmaa käsitellään johdon näkökulmasta.

Tutkimuksessa käsitellään sisäisen valvonnan käsitettä, olennaisimpia sisäisen valvonnan suosituksia ennen Sarbanes-Oxley 404 –lakia, sekä kohdan 404 asettamia vaatimuksia. Empiirisessä tutkimuksessa tarkastellaan yhden yrityksen sisäisen valvonnan käytänteitä ja muutoksia, joita kohta 404 on tuonut case -yrityksen sisäiseen valvontajärjestelmään.

Lähdeaineisto ja aineiston käsittely

Työn tutkimusmetodina on case-tutkimus, jossa tarkastellaan yhtä yritystä. Tutkimuksen aineistoon kuuluu kyselylomakkeet, haastattelut, suora havainnointi, arkistoidut asiakirjat ja dokumentaatio.

Tulokset

Tutkimuksen tulokset osoittavat, että sisäisen valvonnan määritelmä on yhä melko epämääräinen. Määritelmä on muuttumassa kapeasta kohti laajempaa määritelmää. Sisäisen valvonnan ajatellaan olevan osa yrityksen hyvää hallintotapaa. Sarbanes-Oxley laki 404 on ensimmäinen aloite, joka pakottaa yritysten johdon arvioimaan taloudelliseen raportointiin liittyviä sisäisiä kontrolleja.

Syvällisestä case-analyysistä tehdyt tulokset ovat seuraavat: (1) johdon positiivinen asenne sisäistä valvontaa kohtaan on olennainen tekijä tehokkaassa sisäisessä valvontajärjestelmässä, (2) sisäisen valvonnan tarkoitus tulisi viestittää tehokkaasti kaikille työntekijöille, (3) kohta 404 on kasvattanut kontrollien määrää, (4) kohta 404 on johtanut riski- ja prosessikeskeisempään ajattelutapaan.

Tutkimuksessa esitetään case-yritykselle suosituksia, jotka voidaan jakaa kolmeen luokkaan. Ensimmäinen luokka sisältää tekijöitä, jotka mahdollistavat tehokkaamman sisäisen valvontajärjestelmän, ja toinen luokka koskee suositeltuja muutoksia nykyisiin sisäisen valvonnan prosesseihin. Kolmas luokka sisältää suosituksia, jotka liittyvät informaation ja viestintään.

Avainsanat
Sisäinen valvonta, Sarbanes-Oxley –lain kohta 404, COSO viitekehys

CONTENTS

FIGURES

TABLES

ABBREVIATIONS

AAA	American Accounting Association (a sponsoring association of COSO)
AICPA	American Institute of Certified Public Accountants (a sponsoring association of COSO)
ASB	Accounting Standards Board (UK)
CICA	Canadian Institute of Chartered Accountants
CoCo	A Criteria of Control Framework (published by CICA)
COSO	the Committee of Sponsoring Organisations of the Treadway Commission
FASB	Financial Accounting Standards Board in the U.S.
FCPA	the Foreign Corrupt Practices Act of 1977
FEI	Financial Executives Institute (a sponsoring association of COSO)
FRC	Financial Reporting Council (UK)
FSA	Financial Supervision Authority in Finland (RATA)
GASP	Governmental Accounting Standards Board in the U.S.
IAS	International Accounting Standards
IASB	International Accounting Standards Board
IFRS	International Financial Reporting Standards
IIA	Institute of Internal Auditors (a sponsoring association of COSO)
NAA	National Association of Accountants (a sponsoring association of COSO)
OECD	Organisation for Economic Co-operation and Development
OPMAC	Operating Managers' Audit Committee at the case company
RATA	Financial Supervision Authority (FSA) in Finland
SEC	U.S Securities and Exchange Commission
S-O	the Sarbanes-Oxley Act of 2002
S404	Section 404 of the Sarbanes-Oxley Act of 2002
TFV	a true and fair view in financial reporting

1 INTRODUCTION

1.1 BACKGROUND AND MOTIVATION

"In the wake of the financial scandals at Enron, WorldCom, and Tyco International, European chief executives smugly insisted no such fraud could ever occur in Europe. They spoke too soon. The accounting calamity at Italian dairy-foods giant Parmalat has prosecutors scrambling to find out what happened to $8.5 billion to $12 billion in vanished assets. That sum makes Parmalat one of the largest financial frauds in history... "

Parmalat company's financial scandal hit the headlines *"How Parmalat Went Sour: Here's the skinny on Europe's enormous financial scandal"* in Business Week. The company reported 7.6 billion revenue and had 36 000 employees in 30 countries in 2002. The Parmalat case gives a recent example of a significant lack of transparency in financial statements and the misuse of company assets. It is a startling case because Parmalat's managers had falsified the accounts over 15 years (Business Week online 12.1.2004). Although the Parmalat scandal is an alarming case, it is by no means exceptional as fraudulent financial reporting is not just a phenomenon of recent years.

Control activities within organisations were first established to ensure that the companies achieve their objectives and operate according to plans from a management perspective. Over time, the fact that internal control is significant to a company's success was recognised not only by managers of organisation but also by several other parties. Leaders of growing enterprises recognised the need for effective controls when they were faced with larger organisations and an increasing number of employees and activities. It became essential to handle financial and non-financial information in order to monitor activities within the organisation.

Until the middle of the 1970s, internal control activities were emphasised in the system design and auditing and the focus was to improve internal control systems from an auditing perspective (the COSO framework, p.93). However, as a result of the 1973-1976 Watergate investigations, regulatory bodies began to give significant interest to internal control. The

Foreign Corrupt Practices Act of 1977 was enacted. Besides anti-bribery provisions, the act recognised the role of internal control in detecting and preventing fraud in federal legislation for the first time and required a company's management to establish and maintain an adequate internal control system. In 1980s and 1990s, a number of public, private and professional bodies began to publish recommendations and principles regarding an effective internal control system. This attention produced several concepts of internal control and proposed different means to achieve effective internal control. There was, and still is, confusion about the definition of internal control over the years. It will be interesting to examine the definition of internal control and how the concept is linked to a true and fair view in financial reporting, the safeguarding of company assets, or corporate governance. How do different frameworks separate from one another? Additionally, how are the concept of 'control' or 'controls' defined?

In 1992, the Committee of Sponsoring Organisations of the Treadway Commission (COSO) published a report called *"Internal Control – Integrated Framework"* based on an extensive study. Its goal was to improve the quality of financial reporting through a focus on corporate governance, ethical values, and internal control. The framework defined internal control to establish a common definition for different parties and provided a standard against which business and other entities could assess their internal control systems and determine how to improve them. The framework became a common reference point although some argued that COSO made too wide a definition by considering too many organisational measures. According to COSO, internal control is to provide reasonable assurance that a company's financial reporting is reliable and that a company's assets are safeguarded. Internal control is also intended to promote operational efficiency and ensure compliance with applicable laws and regulations. Significant questions arise considering the COSO framework. What are the components of internal control and how are they interrelated? Who is responsible for internal control? How is reasonable assurance measured?

There are national company, accounting, securities markets laws, international regulations and numerous rules of different stock exchanges, which regulate disclosure practices and corporate governance of companies to ensure a true and fair view in financial reporting and safeguarding of a company's assets. Additionally, there are guidance on establishing and maintaining an effective internal control systems. What are the most significant recommendations and what do these various recommendations and principles regulate?

In 2002 the Sarbanes-Oxley Act of 2002 was enacted in the U.S. in response to a number of major corporate and accounting scandals involving well-known corporations in the United States along with other financial scandals throughout the history of several decades. The act imposes federal regulation on the accounting profession and makes significant changes to the responsibilities of corporate managers, auditors and other professionals involved in the financial markets to improve corporate governance, promote ethical business practices and enhance the transparency of financial statements and disclosures. The most significant section of the act from a management perspective, is section 404, which requires a management's assessment of internal control over financial reporting. It will be interesting to examine what the content of the S-O act S404 is in detail? Further, how does the act define the concept of internal control and what does it legislate on maintenance and organising of companies' internal control system? In addition, who are obligated to comply with the S-O act?

Years 2002 - 2004 were the "Years of Internal Control" for many companies, which are in the scope of the Sarbanes-Oxley Act of 2002. It will be interesting to research what kind of changes has section 404 brought to the companies in a context of one case company. How has the case company implemented the act? What do the case company's management and finance personnel consider that the effects of S404 are on the company's internal control system? What challenges has the company faced and what are considered as the benefits of S-O act?

1.2 RESEARCH PROBLEM AND RESEARCH QUESTIONS

The objective of this study is to depict the effect of the Sarbanes-Oxley Act of 2002, S404 on internal control practice. The study aims to describe the effects that the act has on a company's internal control system. The research problem is as follows:

How does Section 404 of the Sarbanes-Oxley Act of 2002 affect internal control practice?

The research problem is explicitly examined from a management's point of view and it is divided in the following research questions:

- *How is internal control defined?*
- *Of what different components does a company's internal control system consist?*
- *What does regulation prior to the Sarbanes-Oxley Act S404 recommend on internal control?*
- *What are the requirements of Section 404 of the Sarbanes-Oxley Act?*
- *How is the internal control system organised and maintained in the case company?*
- *What kind of changes has the S404 brought to the case company's internal control system?*

The fundamental assumptions of this thesis are the concept of 'true and fair view' (TFV) in the financial reporting and the safeguarding of company's assets, which both are the goals of internal control. This thesis outlines its analysis of internal control according to *the COSO framework* (the COSO report "Internal Control – Integrated Framework). From this fact follows that internal control is assumed to consist of five interrelated components: *(1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring.*

1.3 THE SCOPE OF RESEARCH

First, this study examines internal control and the effect of the Sarbanes-Oxley Act S404 on internal control from a management's point of view. The empirical study of the research examines internal control in the light of the case company's business environment. The study does not handle internal control from an external auditor's viewpoint and it does not focus on e.g. issues relating to an auditor independence or an auditor's responsibilities. In addition, it does not examine how the act S404 affects the work of audit committees.

Second, the study is restricted to the title four *"Enhanced Financial Disclosure"* of the Sarbanes-Oxley Act of 2004, and more specifically, only Section 404 *"Management Assessment of Internal Controls"* is examined. The study does not research the content of different national and international accounting standards. These are only discussed shortly in order to introduce the concept of TFV in financial reporting and the safeguarding of company's assets.

Finally, internal control is considered to be a part of corporate governance in this thesis. Corporate governance is covered shortly in this study in order to introduce the role of internal control in a company's governance and to clarify how internal control relates to companies' governance systems.

1.4 THESIS COMPOSITION

This thesis consists of seven chapters. The first chapter is an introduction to the thesis, which introduces the reader to the research study, presenting the research problem and questions, and restricting the scope of research. Key terms and concepts are defined in the chapter.

The second chapter consists of a literature review. It discusses the concept of 'true and fair view' in the financial reporting and covers the most relevant theories and concepts of this study. The chapter also describes the COSO Framework, on which the empirical analysis is based. The third chapter focuses on the regulative framework of internal control by presenting the most important recommendations, regulation and legislation in the United States, in the UK and in Finland.

The fourth chapter presents prior researches relating to management control systems and internal control. The researches of internal control cover areas such as the definition of internal control, demand for the internal control system and demand for the reporting on internal control. The fifth chapter introduces methodology by describing the research method, material used in the study and the design of empirical research.

The sixth chapter covers the empirical analysis of this study. It introduces the case company's business, financial reporting practices and the S404 project and presents the results of in-depth analysis. The seventh chapter summarises the study and presents the conclusions. Recommendations are given to the case company and on future research.

1.5 KEY TERMS AND CONCEPTS

According to the Cadbury report, **Corporate governance** is a system by which companies are directed and controlled. The OECD principles of Corporate Governance define the concept as follows: *"Corporate governance ... involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined."* (1999, p.2).

The COSO framework summarises that **internal controls** *"are put in place to keep the company on course toward profitability goals and achievement of its mission, and to minimize surprises along the way. They enable management to deal with rapidly changing economic and competitive environments, shifting customer demands and priorities, and restructuring for future growth. Internal controls promote efficiency, reduce risk of asset loss, and help ensure the reliability of financial statements and compliance with laws and regulations."* (www.coso.org/publications)

The COSO Framework is a report published by the Sponsoring Organizations of the Treadway Commission (COSO) in 1992. Its goal is to improve the quality of financial reporting through a focus on internal control. The framework defines the internal control concept, describes the five components of internal control, and provides the criteria against which companies can assess and improve their internal control systems. (www.coso.org/publications)

The Sarbanes-Oxley Act of 2002 is a part of the corporate governance regulation and it was enacted in the US on 30th July, 2002. The act applies to the companies whose shares are listed in a securities exchange registered with the SEC and it is intended to protect investors by improving the accuracy and reliability of financial statements. **Section 404** of the act sets the requirements of management assessment of internal controls over financial reporting.

2 LITERATURE REVIEW

Internal control is to provide reasonable assurance that a company's financial reporting is reliable and that a company's assets are safeguarded. An established internal control system is a prerequisite for both a true and fair view in financial reporting and the safeguarding of company assets. It is in the company's best interest to defend and guard its assets from different kinds of losses. There should be appropriate controls in place to protect assets. Reliable financial reporting relates directly to the concept of true and fair in financial reporting. First, literature review introduces the concept of a true and fair view (TFV) or fair presentation (in the U.S.) in financial reporting and safeguarding of company assets by discussing shortly these two goals of internal control in relation to accounting standards, auditing, authorities' oversight and corporate governance. Secondly, it handles management control systems discussed in management accounting literature. Third, the definition of internal control is introduced by discussing the three well-known frameworks of internal control: COSO, CoCo, and the Code of Best Practice. Finally, the COSO framework and the five interrelated components of internal control are handled in detail.

2.1 'TRUE AND FAIR VIEW' AND SAFEGUARDING OF ASSETS

The concept of TFV was introduced into UK legislation in 1947 and further into the fourth EU company law directive in 1974 (Evans 2003). As a result of the Fourth Directive, the TFV had to be presented as a concept in the accounting regulations of all EU member countries. Translations into the official languages of state members were not uniform. Aisbitt and Nobes (2001) researched the implementation of the TFV requirement in Finland, Sweden and Austria, which joined the EU in 1995. For example, article 2 of the Fourth Directive defines an equivalent signifier of TFV as 'right and sufficient picture' in Finnish where as the signifier in the national law is 'right and sufficient information' in Finland. There has been a lot of debate about the right translation into Finnish (see Riistama 1996, Mäkinen 1996, Ekholm and Troberg 1995, for example).

TFV is a basis of accountability. Financial reporting should give a true and fair view of the financial position and financial performance of an entity that enable investors to make right decisions. The prerequisites for TFV and safeguarding of company's assets can be categorised into four different levels as follows: *1. national and international reporting standards, 2. external auditing, 3. the oversight of authorities, and 4. corporate governance.*

2.1.1 National and International Reporting Standards

Both national and international reporting standards and accounting regulation form a basis for a true and fair view in financial reporting. IAS 1.10[1] states that "*financial statements present fairly the financial position, financial performance and cash flows of an entity*" while US regulation states that "*present fairly in conformity with generally accepted accounting principles*" (GAAP). The Finnish Accounting Act (3:2) sets down a rule that a financial statement must give right and sufficient information (and picture) on the company's financial performance and financial position.

According to IAS 1.13, a departure from IFRS standards is acceptable only in extremely rare circumstances in which the compliance with IFRS conflicts with providing information according to the TFV requirement. Paragraph 13 specifies the required disclosures when an entity departs from IFRS standards. Contrary to IAS requirements, there is no concept of a true and fair view override in U.S. GAAP. As mentioned earlier, TFV or rather 'fair presentation' is dependent on generally accepted accounting principles. As Evans (2003) points out, the concept has no legal significance in the U.S. regulation.

There has been a lot of discussion about the overriding rule of TFV over the years. Alexander (1993) suggests that TFV is an overriding rule and is always relevant either directly or through its influence on accounting regulation. Also Aisbit and Nobes (2001) support the overriding rule by arguing that TFV is more important than any particular rules of practice and therefore the requirement for the rules is to be broken if this is necessary in order to portray reality. However, according to Van Hulle (1993), the use of this option should be limited to exceptional cases in order to avoid the abuses of the TFV override.

---

[1] IAS 1: Presentation of Financial Statements

2.1.2 Auditing

To clarify the relationship between TFV and auditing, Ekholm and Troberg (1998) state a relevant question by asking what are the mission and reporting obligations of an auditor?. They refer to Bryer's study (1993), in which the author quotes the chairman of the London Stock Exchange by writing *"...upon the auditors as being a great safeguard of the interests of investors ..."* (Select Committee 1896, 743-44). Bryer also writes that the 1900 Act in the UK *"required the auditors to report whether in their opinion the balance sheet was properly drawn up so as to exhibit true and correct view of the state of the company's affairs as shown by the books of the company"* and he states that the act placed a special burden on auditors. The Finnish Auditing Act §17 states that auditors have to give a statement whether a company's financial statements give a true and fair view of the results of operations as well as of the financial position.

Parker and Nobes (1991) examined the operational meaning of TFV on large auditing firms. They conclude that the TFV requirement is used by the auditors to give support to auditors' views in areas where there is not yet an accounting standard. They further present that less often TFV is, however, used to modify rules already established (p.357). Contrary to Parker and Nobes, Williams (1985) argues that the TFV requirement exists mainly for the benefit of an auditor.

McNamee (1997) discusses SAS[2] No. 55 "Consideration of Internal Control in a Financial Statement Audit" issued by the AICPA, which requires auditors to assess a company's control environment. He further states that auditors have a responsibility to consider how management safeguards a company's assets. McNamee presents a relevant question that auditors must answer: *"How could loss or misappropriation of assets cause the financial statements to be materially misstated?* He states that identifying potentially vulnerable assets is one part of the answer. The other is that auditors have to find a link between those assets and possible material misstatements of financial statement assertions. If a link could exist, the auditors should determine whether management has controls in place to safeguard assets. According to Recommended Auditing Practices 2003 in Finland (p.130), auditors should

[2] Statement of Accounting Standard (Auditing)

learn about a company's control environment and internal control system in order to be able to assess a management's attitude towards internal controls.

According to Curtis and Wu (2000), SAS No. 55 describes internal control in terms of three major components: control environment, accounting system, and control procedures. The authors continue that in 1995, the AICPA adopted the COSO's definition and five components of internal control and issued SAS No. 78 to supplement SAS No. 55. These five components are control environment, control activities, risk assessment, information and communication, and monitoring that will be introduced later in this study.

2.1.3 Oversight of Authorities

As discussed, the concept of TFV was introduced into the EU legislation in the 1970s. The fourth EU company law directive states only that financial reporting shall give a true and fair view. Ekholm and Troberg (1998) summarise that the accounting authorities of the EU seem to be quite non-specific on the issues of the objectives of financial reporting and specifically, on the issues of information qualities set by the TFV requirement.

The International Accounting Standards Board (IASB) has no authority to require compliance with its accounting standards. However, the European Union sets a requirement that the management of European publicly traded companies has to prepare their financial statements in accordance with International Financial Reporting Standards (IFRS) starting from year 2005 at the latest. Furthermore, IFRSs require that financial statements should fairly present or give TFV of a company's financial position at the end of the year, the result of its operations and cash flow of the year.

The Financial Reporting Council (FRC) is an independent regulator for corporate reporting and governance in the UK. Accounting Standards Board (ASB) as an operating body of FRC issues accounting standards and it is recognised for that purpose under the Company Act 1985. Also ASB states clearly the requirement of the TFV (www.asb.org.uk/asb). Established in 1990 as a subsidiary of the FRC, The Financial Reporting Review Panel considers whether the annual accounts of public and large private companies comply with the Companies Act

1985 including applicable accounting standards. The Panel has an authority to confront company's management about obvious departures from the accounting requirements and if not satisfied, persuade them to adopt a more appropriate accounting treatment. If managers refuse to make corrections, the panel can exercise its power to secure the necessary revision of the original accounts through a court order. (www.asb.org.uk/frrp)

The U.S. Securities and Exchange Commission (SEC) is the primary overseer and regulator of the U.S. securities markets. The mission of SEC is to protect investors and maintain the integrity of the securities markets. SEC has a statutory authority to establish financial accounting and reporting standards for publicly held companies under the Securities Exchange Act of 1934 and it has an authority to bring civil enforcement actions against individuals and companies that break the securities laws. The latest standard established by SEC is the Sarbanes-Oxley Act of 2002, which requires an annual assessment of internal control to ensure financial statement accuracy and safeguarding of assets. In addition to SEC, there are self-regulatory organisations, such as stock exchanges, which oversee the securities markets. Companies listed on the Nasdaq Stock Market or NYSE[3] are also required to meet also the marketplace rules.
(www.nyse.com/regulation and www.nasdaq.com/about/LegalCompliance.stm)

Since 1973, the Financial Accounting Standards Board (FASB) has been the designated organisation in the private sector for establishing standards of the preparation of financial reports in the U.S (the GASP for the state and local governmental accounting and financial reporting). The objective of these standards is to provide "*credible, transparent and comparable financial information on which investors, creditors, auditors and others can rely on*" and so, secure the efficient functioning of the economy. FASB is officially recognized as authoritative by the Securities and Exchange Commission and the American Institute of Certified Public Accountants (www.fasb.org/facts).

Rahoitustarkastus (RATA) is the Financial Supervision Authority (FSA) in Finland, which oversees financial markets and parties in these markets. Its objective is to ensure financial stability and maintain public confidence in financial markets. It has an authority to give a

[3] New York Stock Exchange

public notification or warning, impose a conditional fine or to make a request for police investigation. However, FSA does not have such a strong enforcement authority as SEC has in the U.S. Helsinki Stock Exchange has also published the Rules of the Securities Exchange for listed companies.

2.1.4 Corporate Governance

Recommendations on corporate governance has drawn more and more public attention. Corporate governance relates to reliable financial reporting and safeguarding of company assets. According to Määttä (2000), a mere numerical financial information is not adequate for investors anymore but they want to get extensive information on management, the administration systems and the functionality of these systems.

In 1992, Cadbury Committee's pioneering report "the Code of Best Practice" on corporate governance was published in the UK. This report lists nineteen recommendations relating to a company's board of directors, external auditing, financial reporting and control systems. Although the recommendations are not mandatory, e.g. London Stock Exchange requires listed companies to state in their annual statement whether these recommendations are followed or not (www.indiainfoline.com/nevi/cadb.html). The committee states that *"a basic weakness in the system of financial reporting is the possibility of different accounting treatments being applied to essentially the same facts, with consequence that different results or financial positions could be reported, each apparently complying with the overriding requirement to show true and fair view."* It argues that the overriding rule may cause uncertainty and manipulation (para. 4.47) but considers TFV in financial reporting as a basic principle (para 4.51).

Määttä (2000) presents an interesting question, whether TFV is an accounting, operational, societal, juridical or economical issue? Accounting practices are prepared by individuals in a certain environment and accounting rules are under constant development. He quotes Weber (1993) by writing: *"In the end, the location of the new economy is not in the technology, be it the microchip or the global telecommunication network. It is in the human mind."* With this quotation Määttä highlights that considering TFV, accounting, financial reporting or other technical system does not solve the problem of true and fair information – it is the responsibility of people. Corporate governance and the role of internal control in governance systems will be discussed later in this study.

2.2 MANAGEMENT CONTROL SYSTEMS

According to Drury (2000), control is the process of ensuring that a company's activities conform its plan and that its objectives are achieved. He highlights that there can be no control without objectives and plans because these specify the desirable behaviour and set out the procedures that should be followed by the organisation in order to ensure that a company is operating in a desired manner. Drury refers to Drucker (1964), who clarifies the difference between 'controls' and 'control'. Drucker states that controls are purely a means to an end; the end is control. In other words, controls are measurement, information, methods and procedures that direct employees towards the achievement of the company's objectives, where as control means direction.

Drury classifies controls into three categories that have been adopted from Merchant (1998) and Ouchi (1979):

1. action or behavioural controls;
2. personnel, cultural and social controls;
3. results or output controls

Drury states that the action and behavioural controls are used when managers know what actions are desirable. These controls are appropriate where cause-and-effect relationships are well understood so that if the correct means are followed, the desired outcomes will occur. Behavioural controls are e.g. superior observing the actions of individuals as they are working, where as action controls relate to situations, in which the actions themselves are the focus of controls. According to Merchant (1998), action controls include behavioural constraints, pre-action reviews and action accountability. Behavioural constraints include physical constraints such as computer passwords that restrict accessing or updating information from unauthorised personnel, or administrative constraints e.g. ceilings on the amount of expenditure of managers. Pre-action reviews can be different kinds of approvals of action plans, while action accountability involves defining actions that are acceptable or unacceptable, observing the actions and rewarding or punishing. These controls can be e.g. work rules and procedures or company code of conduct.

Merchant (1998) defines that personnel controls are helping employees do a good job by building on employees' natural tendencies to control themselves. These controls ensure that personnel has both the capabilities in terms of intelligence, qualifications and experience, and the resources to do a good job. He identifies three major methods of implementing personnel controls: selection and placement, training and job design, and the provision of necessary resources. Ouchi defines that social controls can be viewed as corporate cultures, in which there is the selection of people who have been socialised into adopting particular norms and patterns of behaviour. Drury clarifies that cultural controls represent a set of values, social norms and beliefs that are shared within the whole organisation and that influence the actions individuals. He also takes up an important point of recent years working practices by noting that nowadays managers are relying on people closest to the operations and customers to take actions without superiors' authorisation. This approach is known as employee empowerment and it involves control being transferred more to different levels within an organisation. Delegation of control may have both positive and harmful side-effects. Empowerment may result in a quicker decision making and actions. On the other hand, it may increase the risk of a company not achieving its objectives if authorised individuals are not acting in the company's best interests.

According to Drury (2000), output or results controls involve collecting and reporting information about the outcomes of work effort. He notes that accounting systems can be described as a form of output controls and that they are mostly defined in monetary terms such as revenues, costs, profits and ratios. Output or results controls can also be non-accounting measures e.g. the number of customer deliveries on time as a percentage of total deliveries. Drury summarises that result controls involve that performance measures and targets are established and that performance is measured and rewards or punishment provided. Without a pre-set performance target individuals do not know what to aim for.

Different kind of controls involve advantages and disadvantages. Drury refers to Merchant

(1998), who suggests that managers should first consider whether personnel or cultural controls will be sufficient because these controls have relatively few harmful side-effects. Merchant notes that in small organisations they may be effective without the need to supplement them with other controls. However, he points out that these controls are appropriate only if the people in their particular roles understand the requirements, are capable of performing well and are motivated to perform well. According to Drury, action controls are the most effective form of control because there is a direct link between the control and the action and there is also a high probability that desirable outcomes will occur. He points out that, on the other hand, action controls may discourage creativity and are unsuitable in a changing environment. Therefore, these controls often are applicable to only highly routinised jobs and they are suited to stable situations.

According to Drury (2000), the major advantage of result controls is that senior managers do not have to know the means required to achieve the desired results. The focus on outcomes gives individuals the freedom to determine how they can best achieve the outcomes. On the other hand, there may be a danger that employees will concentrate only on what is monitored by the control system and they will maximise their individual performance without considering whether their actions contribute to the company's objectives. In addition, as Drury notes, result controls tend to focus on controlling behaviours that are quantifiable and measurable.

Horngren and Sundem (1993) concentrate on financial controls by defining a management control system as follows: *"a logical integration of management accounting tools to gather and report data and to evaluate performance"*. They state that information to support the management control system often comes primarily from the organisation's financial accounting system. The authors point out that too often financial accounting systems focus on technical details of data processing, external financial reporting, compliance with legislation or detection of fraud, and do not emphasise employee motivation, performance evaluation, or management decision making. Thus, Horngren and Sundem state that the management control system should be designed to improve the decision making in the company. However, they emphasise that the management control system should also focus on organisational goals and objectives and foster goal congruence[4] and managerial effort. Managerial effort is defined as exertion toward a company's objectives that results in efficiency and effectiveness.

According to Horngren and Sundem (1993), an internal control system consists of methods and procedures to both *prevent* and *detect* errors and irregularities and to *promote* operating efficiency. The authors note that a management control system includes *administrative controls*, such as budgets for planning, controlling, and evaluating operations, and *accounting controls,* such as separating of duties of the person who counts cash from duties of the person who has access to the accounts receivable records.

2.3 DEFINITION OF INTERNAL CONTROL

There are many different control mechanisms used in organisations. The previous chapter handled management control systems that represent only one aspect of the various control mechanisms that companies use to control their managers and employees. The approach of management accounting toward control and controls emphasises that the management control systems are tools for decision making and performance evaluation and that the management control systems focus on financial information and financial controls. Next, the control systems will be discussed from a broader view and the definition of internal control will be introduced.

2.3.1 Corporate Governance: The Role of Internal Control

The shareholders' role in governance is to appoint a company's board of directors and auditors. The board is responsible for the company's governance. According to Ernst & Young (2003), good governance is about acting openly, honestly and in such a responsible way that a company is organised and registered according to laws and regulation. It is organised and its operations are planned, directed and carried out according to the professional requirements, which are approved and applied by the board of directors. The company's assets are administered correctly and its governance is under sufficient internal control.

---

[4] Goal congruence exists when individuals and groups aim at the same organisational goals.

The Cadbury Committee's report *"Code of Best Practice"* presents that corporate governance comprises of three factors. The first factor is the structure and responsibilities of the board of directors and the second is the role of auditing in corporate governance. The last factor covers companies' supervision mechanism, financial reporting and the shareholders' rights. The committee considers (p.41) that an effective internal control system is an essential part of a company's efficient management. OECD takes a more broader view than the Cadbury Committee. *"OECD Principles of Corporate Governance"* (1999) state that corporate governance also covers factors such as management incentives, corporate awareness of environmental and societal issues. OECD considers that creditors play an important role in the governance system and have a potential to serve as external monitors over company performance. Also *"Corporate Governance Recommendations for Listed Companies"* in Finland (2003) consider that good governance includes internal control, risk management and internal audit.

To summarise, the key components of effective corporate governance are the board of directors including an audit committee, a company's management, internal and external auditing, and a company's stakeholders. Internal control is closely related to these key components and a company's management, supervised by the board, is responsible for organising and maintaining the internal control system. In practise internal controlling is performed as an ongoing process by a company's personnel. The mission of internal auditors is to assess and ensure that the company's internal control processes are in place and that the company operates according to its objectives. External auditors and other stakeholders such as creditors, authorities, and customers are not responsible for a company's internal control and they are not considered to be a part of the internal control system. However, these parties have an influence on whether the company achieves its objectives.

2.3.2 What is Internal Control?

There has been confusion over the exact meaning and the scope of *internal control* and the definition has evolved over time. According to SEC, the term was historically applied mostly within the accounting profession. SEC notes that the early attempt (e.g. AICPA in 1949) to define the term clarified only what different factors of a company's internal control should be considered in external auditing. In 1949, AICPA's report *"Internal Control - Elements Of a Coordinated System and Its Importance to Management and the Independent Public Accountant"* clarified internal control as follows:

> "the plan of organisation and all of the coordinate methods and measures adopted within a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies."

Later, AICPA divided the controls relevant to audit into *internal accounting controls* and non-accounting controls i.e. *administrative controls*. (SEC Final Rule 5.6.2003, Release No. 33-8238).

In 1992 COSO published a report *"Internal Control – Integrated Framework"*. This report is widely considered as a common framework for defining internal control. For example, AICPA incorporated the definition of internal control presented by the COSO in Statement on Auditing Standards No. 78 (SEC Final Rule 5.6.2003). The framework states (p. 3) that internal controls are put in place to keep the company on course toward profitability goals and achievement of its mission, and to minimise surprises along the way. According to COSO, internal controls enable management to deal with rapidly changing economic and competitive environments, shifting customer demands and priorities. Internal controls promote efficiency, reduce risk of asset loss, and help ensure reliability of financial statements and compliance with laws and regulations.

The second framework "the Code of Best Practice" developed by the Cadbury Committee was published in the UK in 1992. The report also takes a broad interpretation of control but focuses on the financial controls. According to the code, financial controls should provide reasonable assurance of effective and efficient operations, reliability of financial information and compliance with the laws and regulations. Although these objectives are very similar to the objectives of the COSO framework, the code covers financial aspects only. The Code of Best Practice is discussed thoroughly in the regulative framework of this study.

The third framework is called *"A Criteria of Control Framework"* (CoCo) and it was published by the Canadian Institute of Chartered Accountants (CICA) in 1995. CoCo defines that control includes all elements of an organisation: its resources, systems, processes, culture, structure and tasks. These elements together support people in the achievement of the company's objectives. A control is effective if it provides reasonable assurance that the organisation will achieve its objectives reliably (Jackson and Livick-Chan, 1999). Thus, the internal control system is also defined broadly in the CoCo framework. CICA published the "Guidance on Control" (1995), in which it classifies the criteria of control under the following components: (1) purpose, (2) commitment, (3) capability, and (4) monitoring and learning. Next, the criteria is covered shortly based on Cooper's and Gendron's article (2001).

According to Cooper and Gendron, *purpose* means that people in the organisation should operate according to the company's objectives. These objectives should be clearly formulated and communicated. *Commitment* involves that the people within the organisation need a sense of commitment in order to perform their job well over time. Therefore, shared ethical values should be established, communicated and practiced throughout the organisation. According to Cooper and Gendron, CICA's Guidance on Control note that high ethical values play a critical role in the internal control system because they determine the way people operate. The criterion of *capability* covers competence, skills, and open communication in the organisation. If personnel is capable of performing appropriately, they have to be supported by resources including information systems. The CoCo framework highlights that decision-makers should be provided with relevant and timely information. The last criterion, *monitoring and learning* suggests that companies should monitor their performance in order to learn how to perform tasks better and what changes should be made. The objectives should be put into practice through measurable performance targets and indicators. Actual performance should then be monitored against these targets.

Thus, the Code of Best Practice and the CoCo framework include several issues that are also covered in the COSO framework. The frameworks define internal control broadly and discuss issues such as commitment to a company's objectives, competence and skill, effective and efficient operations, reliable financial reporting, compliance with laws and regulation, ethical values and communication. Because of the fact that the COSO framework is considered as a common reference point, the framework will next be discussed in detail.

2.4 COSO FRAMEWORK

In 1992, Committee of Sponsoring Organizations of the Treadway Commission (COSO) published a report *'Internal Control – Integrated Framework'* based on an extensive study, which consisted of seven phases. These phases included literature search, 45 one-on-one interviews, 522 responses to a questionnaire, 8 workshops, public exposure (40,000 copies distributed and 211 comment letters received), field tests in five public companies, and additional exposure and meetings. Different parties, such as corporate executives, legislators, regulators, academics and auditors participated to the study. The goal of the report was to improve the quality of financial reporting through a focus on internal control. The framework defines and describes internal control in order to establish a common definition serving the need of different parties, it provides a standard against which business and other entities – large or small, in the public or private sector, for profit or not – can assess their internal control systems and determines how to improve them. (Internal Control – Integrated Framework, p.3).

According to the framework (p.13), ***internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following three categories:***

(1) Effectiveness and efficiency of operations
(2) Reliability of financial reporting
(3) Compliance with applicable laws and regulations.

This definition reflects certain fundamental concepts. First of all, internal control is *a process*. Contrary to Drucker's definition, the framework emphasises that internal control is a means to an end, not an end in itself. Internal control should be a part of the basic management processes of planning, executing and monitoring and should be integrated with them. Second, internal control is effected by *people*. As a result, it must be realised that internal control is not merely policy manuals and forms, but people at every level of an organisation play an essential role in it. People establish the company's objectives and put control system in place. Similarly, internal control affects people's action. Internal controls include that people have to know their responsibilities and limits of authority.

Third, internal control can be expected to provide *reasonable assurance*, not absolute assurance, to a entity's management and board. An internal control system naturally involves limitations, which affect the likelihood of achievement. These limitations may include faulty human judgements in decision-making or human failures such as simple error or mistake. Persons responsible for establishing controls have to consider relative cost and benefits and controls can be circumvented by collusion of two or more people. In addition, management has the ability to override the internal control system. COSO notes that even an effective internal control can only help a company achieve its basic business objectives by providing management information on a company's progress, or lack of it. However, internal control can not change a poor manager into a good one, or can not predict shifts in government policy and competitors' actions. Also economic conditions can be beyond management's control.

Finally, internal control is geared to the achievement of *objectives* in one or more separate but overlapping categories. Every company establishes its mission and objectives, which it wants to achieve, and creates strategy for achieving them. Objectives may be set to the company as a whole or they can be targeted to specific activities within the organisation. The framework categorises objectives into operations, financial reporting and compliance. The first category relates to a company's basic business objectives. These objectives involve performance and profitability goals, as well as safeguarding both tangible and intangible assets. The second category covers the preparation of reliable published financial statements and the third category deals with complying with those laws and regulations to which the company is subject to.

According to the framework (p. 20), the internal control system operates at different levels of *effectiveness* and internal control effectiveness is a state or condition of the internal control process at one or more points in time. Internal controls are effective in each of the above listed three categories, respectively, if the board and management have reasonable assurance that (1) they understand the extent to which the company's operations objectives are being achieved, (2) the published financial statements are being prepared reliably, and (3) applicable laws and regulations are being complied with. Determining whether a certain internal control system is effective needs an assessment of whether the five components of internal control are present and functioning effectively.

COSO breaks down internal control into five interrelated components. According to the framework (p.16), these components are derived from the way management runs a business, and are integrated with the management process. These five components are:

1. **Control Environment**
2. **Risk Assessment**
3. **Control Activities**
4. **Information and Communication**
5. **Monitoring**

According to the framework (p.18), there is a direct relationship between the objectives, which are what a company strives to achieve, and the components, which represent what is needed to achieve the objectives. The relationship can be depicted with a three-dimensional matrix (Figure 1), which includes the three objectives categories, the five components and a company's units or activities. The components cut across the whole organisation and apply to all objectives categories. For example, information is needed to effectively manage business operations, prepare reliable financial statements and determine compliance or all five components must be present and functioning effectively to achieve operational objectives.

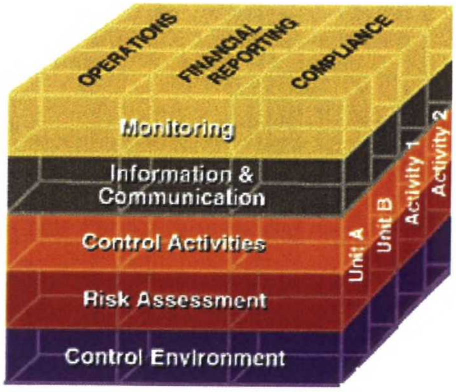


Figure 1: The relationship between the objectives and the components of the COSO framework

2.4.1 Control Environment

The control environment is a key component of a company's internal control and it influences control activities, information and communication systems, and monitoring activities. According to the framework (p.23), *"control environment sets the tone of an organisation, influencing the control consciousness of its people"*. Control environment factors include: the integrity, ethical values and competence of the company's people, management's philosophy and operating style, the way management assigns authority and responsibility, and organises and develops its people, and the attention and direction provided by the board of directors. The control environment is influenced by the company's history and culture.

Integrity and Ethical Values

The framework notes that a company's objectives and the way they are achieved are based on preferences, value judgements and management style. These factors reflect management's integrity and its commitment to ethical values. "The tone at the top" is a major factor in creating positive control environment. The effectiveness of internal controls can not rise above the integrity and ethical values of the people within an organisation, who create, administer and monitor controls. Integrity and ethical values are significant elements of the control environment. The framework states that ethical behaviour and management integrity are a product of the corporate culture, which includes ethical and behavioural standards and communication and reinforcement of these standards. COSO emphasises that official policies state what management wants to happen, where as corporate culture determines what actually happens, and which rules are obeyed, compromised or ignored.

Individuals may take dishonest, illegal or unethical actions if their organisation gives a strong incentives or temptations to do so. For example, emphasis on "results" i.e. making revenue or profit, especially in the short term, promotes an environment in which individuals are trying to achieve the targets in every possible way and the price of failure becomes very high. According to the framework, incentives can be high performance-dependent rewards or pressure to meet unrealistic short-term results. Temptations may include e.g. high decentralisation or poor segregation of duties, which can lead to stealing of company's property or concealing weak performance.

The most effective way to foster ethical behaviour within the organisation is by example. As the framework notes, people imitate their leaders and they are likely to develop the same attitude toward internal control as the management. Besides setting a good example, top management should communicate the company's values and behavioural standards to employees. According to COSO (p.26), companies have adopted a formal code of corporate conduct along with necessary communications channels and monitoring. The framework emphasises that it is also important to have penalties for employees who violate such code and create mechanisms that encourage employees to report suspected violations.

Commitment to Competence

According to the framework, management has to specify the competence levels for particular jobs and to translate those levels into required knowledge and skills. Knowledge and skills naturally depend on an individuals' intelligence, training and experience. Competence has a direct influence on internal controls because it determines how well the job is done. There is often a trade-off between competence and cost. Management has to also consider the nature and degree of judgement to be applied to a particular job because there can be a trade-off between the extent of supervision and the competence level of the individual.

Board of Directors and Audit Committee

The company's board of directors and audit committee influence significantly "the tone at the top" (p.26). A strong, competent and active board and audit committee have an effect on the control environment. The extent by which the board and audit committee handle difficult questions regarding plans and performance with the management affects control environment. Other factors include independence from management, experience of the members and the appropriateness of its actions. In addition, the cooperation of the board and audit committee with internal and external auditors affect control environment.

Management's Philosophy and Operating Style

According to the framework (p.27), management's philosophy and operating style influence the way the company is managed and what kinds of business risks are accepted. A company with successful risk taking may have a different view of internal control than a company, which has faced regulatory or economic consequences as a result of venturing into a dangerous territory. An informally managed company may control operations by having a lot of informal face-to-face meetings, while a formally managed company may rely more on written policies, performance indicators and exception reports. Management philosophy and operating style also include attitudes toward financial reporting. Financial reporting requires a conservative or aggressive selection from available alternative accounting principles.

Let's take an example. Consider that a company's internal controls require that the board of directors shall approve all significant decisions made by the CEO, and that the philosophy of the CEO is that: "I alone know what is best for the organisation". Due to the CEO's philosophy, it is likely that the criterion for advancement within the organisation is personnel's loyalty to the CEO, and that senior management's information to the board is tightly controlled and presented in the way the CEO requires. Therefore, the activity-level controls may look good because all major decisions probably have an approval from the board. However, effective control environment is not in place because the CEO overrides internal controls. It is not enough that the activity-level controls are followed because they are not giving a true picture of an organisation. This example captures the fact that a control environment is a key factor in the internal control system.

Organisational Structure

An entity's activities are organised to carry out the strategies to achieve entity-wide objectives (p.28). An organisational structure provides the framework in which the entity's activities are planned, executed, controlled and monitored. According to COSO, key aspects of a relevant organisational structure include defining of authorities and responsibilities and establishing appropriate lines of reporting. Some organisations are centralised, others decentralised. Some have direct reporting relationships, others are a matrix organisation. The framework emphasises that a company's organisational structure should support its needs. For example, a highly structured organisation, including formal reporting lines and responsibilities, may be appropriate for a large entity with numerous operating units and foreign operations. However, it may harm a small entity's operations.

Assignment of Authority and Responsibility

Authority and responsibility is usually cascaded to different levels at the organisation. This includes assignment of authority and responsibility for operating activities, and defining reporting relations and authorisation protocols (p.28). Individuals are encouraged to use initiative in addressing issues and solving problems. Delegation of authority –empowerment– means that control of business decisions is given to a lower level in the organisation. A critical challenge is to delegate only to the extent that is required to achieve a company's objectives. This requires that risk acceptance is based on risk assessment to make good business decisions.

According to the framework, another challenge is to make sure that all employees understand the company's objectives. It is important that each individual knows how his or her actions interrelate and contribute to the achievement of the company's objectives. The control environment is influenced by the extent to which the people feel that they will be held accountable. This also applies to the chief executive, who has ultimate responsibility for all activities within the organisation including internal control system.

Human Resource Policies and Practices

Human resource practices send messages to employees regarding expected levels of integrity, ethical behaviour and competence (p.29). These practices relate to hiring, orientation, training, evaluating, promoting, and compensating. For example, a standard for hiring most qualified individuals indicates a company's commitment to competent and trustworthy people. Recruiting practices that include in-depth employment interviews and presentations on the company's history, culture and operating style send a message that the company is committed to its people. Training policies illustrate expected levels of performance and behaviour and competitive compensation programs motivate to outstanding performance. Disciplinary actions send a message that violations of code of conduct will not be tolerated.

2.4.2 Risk Assessment

According to the framework (p.33), every company faces a variety of risks from external and internal sources that have to be assessed. Risks have an effect on a company's ability to survive, compete successfully in the market, sustain economic growth, and assure the quality of product and services. It is not possible to keep risks at a zero level and therefore, management has to determine the acceptable risk level and stay within the limits. A precondition to risk assessment is the establishment of a company's objectives, which are linked at different organisational levels. The framework notes that risk assessment means that risks, which are relevant to the achievement of the objectives, are identified and analysed. An assessment is a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions are under constant change, also these changes have to be assessed and mechanisms are needed to identify and deal with the special risks associated with these changes.

Objectives

Establishment of a company's objectives is a precondition to risk assessment. Objective setting can be a highly structured or an informal process. Objectives may be clearly defined or they can be implicit, such as "to continue at past level of performance". The framework notes that entity-level objectives are linked and integrated with a more specific objectives of various activities within the organisation such as sales, production and administration. Setting objectives at the entity or activity level, helps a company determine critical success factors, which have to go right in order to meet the goals. Objectives can be categorised into basic business objectives, financial reporting objectives and compliance objectives.

Risks

The framework states (p.39) that the process of identification and analysing risks is an ongoing iterative process, which is a critical component of an effective internal control system. Management must carefully pay attention to risks at different organisation levels and take actions to control them. Regardless of the fact, whether an objective is clearly defined or implicit, a risk assessment process should consider risks that may occur. It is important that risk identification is comprehensive and it should consider all significant interactions (products, services and information) between a company and relevant external parties (p.40). Risks at the entity-wide level can arise from internal and external factors. External factors may include e.g. technological developments, changing customer needs and expectations, competition, new legislation and regulation, economic changes, and natural catastrophes. Internal factors may be e.g. a disruption in information systems, poor quality of personnel hired and methods of training and motivating, changes in management responsibilities, or an ineffective board or audit committee.

After the company has identified entity-wide and activity risks, the risks need to be analysed (p.42). The framework notes that methods for analysing risks can vary but the process usually includes the following steps: estimating the significance of a risk, assessing the likelihood of the risk occurring, and considering the means of managing the risk. A risk that does not have a significant effect on the company and that has a low likelihood of occurrence does not require serious concern. On the other hand, a significant risk with a high likelihood of occurrence should be carefully assessed. It is important that the analysis is rational and careful.

Once identified risks are analysed, management has to consider how the risks should be managed. Some actions may eliminate the risk or offset its effect if it does occur. These actions may include hedging financial exposures and obtaining adequate insurance coverage. Numerous actions can be taken to reduce the significance or likelihood of the risk occurring. These actions may include identifying alternative supply sources or improving training programs, for example.

The framework reminds (p.43) that economic, industry and regulatory environments change and companies' activities evolve. Internal control can be effective in a some point of time but it may not necessarily be effective in changed conditions. These conditions may include e.g. changed operating environment, new personnel, new information system, rapid growth, new technology or new products and activities, or corporate restructuring. Managing change requires management's careful attention and there should exist mechanisms to identify and react to changes that may have a dramatic effect on the company.

2.4.3 Control Activities

According to the framework (p.49), *"control activities are the policies and procedures, which help ensure that management directives are carried out within the organisation. They help ensure that necessary actions are taken to address risks to achievement of a company's* *objectives.*" Control activities occur at all organisational levels. Control activities include e.g. approvals, authorisations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties. Control activities can be divided into three categories, based on the company's objectives to which they relate: operations, financial reporting and compliance.

The framework categorises controls differently from Drury, Merchant and Ouchi. According to COSO, there are different types of control activities such as preventative controls, detective controls, manual controls, computer controls or management controls. Control activities can be typed by specified control objectives, such as ensuring completeness, and accuracy of data processing. The framework presents (p.50) that there are certain control activities commonly performed by the people at various levels in organisation as follows:

1. Top Level Reviews – Reviews made of actual performance versus budget, forecasts, prior periods, and competitors.

2. Direct Functional or Activity Management – Managers running functions or activities review performance reports.

3. Information Processing – A variety of controls performed to check accuracy, completeness and authorisation of transactions.

4. Physical Controls – Equipment, inventories, securities, cash and other assets are secured physically, and periodically counted and compared with amounts shown on control records.

5. Performance Controls – Relating different set of data (operational or financial) to one another, together with analyses of the relationship and investigate and corrective actions, serve as control activities.

6. Segregation of duties – Duties are divided or segregated among different people to reduce the risk of error or inappropriate actions.

In addition, the framework discusses controls over information systems (p.52) and notes that with widespread reliance on information systems, control activities are needed over all these systems. COSO divides information systems control activities in two groups: general controls and application controls. General controls include control over data centre operations, system software acquisition and maintenance, access security, and application system development and maintenance. Application controls help ensure the completeness and accuracy of transactions processing, authorisation and validity. The framework reminds that particular attention should be paid to an application's interfaces. For example, these situations may include that data is transferred from a specific application (e.g. Excel) to a main information system to e.g. general ledger accounts. General and application controls serve to ensure that the completeness, accuracy and validity of the financial and other information in the system.

According to the framework (p.51), control activities include two elements. A policy describes what should be done and a procedure is a control activity itself. Policies can be written or communicated orally. A procedure will not be useful if it is performed mechanically without the consideration of purpose of the procedure. Consider a case where a customer is asked to show his or her identification (the latter part of the social security number) when the payment is done with a credit card. If identification is not compared to the cardholder's personality at all, control activity is just mechanical and useless control activity.

The framework states that along with assessing risks, management should identify and put in practice control activities needed to address the risks. Control activities are a part of the process by which a company strives to achieve its objectives. The framework highlights that they should not exist simply for their own sake or because it seems to be the right thing to do.

2.4.4 Information and Communication

COSO emphasises (p.59) that pertinent financial and non-financial information should be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems should produce reports, which contain operational, financial and compliance-related information, and which make it possible to run and control the business. The framework notes that they should deal with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting.

Information is needed at all organisational levels to run the business and to achieve the objectives. Information is applied to build up financial reports, in operational decision-making, and in monitoring of activities. Information systems store, maintain, process and report information and they include information produced both within the organisation and outside the organisation. To be effective, information system should process and report information on time and in a way that benefits the organisation in controlling activities. Nowadays, information systems are an integral part of organisation's daily operations and they are utilised not only to gather information, but to implement strategic plans. Strategic use of information systems helps controlling of business activities by monitoring and registering activities in real time within the organisation with a lot of different information systems.

It is important that reports consist of sufficiently appropriate and correct information to support an efficient internal control. *Considering the quality of information, the following questions are relevant: Is the needed information there? Is it there when required? Is it the latest information available? Can it be obtained easily by appropriate parties?* Because also information systems are a part of internal control system, it is necessary to control them. As the framework notes (p.62), the quality of system-generated information affects management's ability to make appropriate decisions in managing and controlling the company's activities.

Effective communication is needed – flowing down, across and up the organisation. The framework emphasises (p.59) that *"all people within the organisation must receive a clear message from top management that control responsibilities must be taken seriously"*. This applies particularly to financial managers and to people who have important assignments. The framework also notes that all people have to understand their own role in the internal control system. It is also essential that individuals know how their activities relate to the work of others. All personnel must know the conduct that is expected from them and what kind of behaviour is acceptable and what is not. In addition, they must have a means of communicating significant information upstream. Employees in operations deal with critical issues every day and they have the best position to detect the problems. In order to get this information to higher level within the organisation, there has to be up-front communication and superior's interest to listen (p. 64). Usually employees quickly notice implicit and explicit messages about superior not having time or interest to handle the problem, which they have brought out.

The framework states (p.65) that communication between the management and the board of directors and its committees is critical. Management has to keep the board up to date on performance, development, risks, major initiatives, and any other relevant events and issues. The better the communications to the board, the more effective it can be in carrying out its oversight responsibilities. The framework also notes that there needs to be effective communication outside. This means external parties, such as customers, suppliers, regulators and shareholders. Communications from external parties may provide information on the functioning of internal control system. External auditors' understanding of a company's operations and control systems provides management and the board important control information. Regulators report results of compliance reviews that may provide information about control weaknesses. Also feedback from customer complaints or inquiries about shipments point to operating problems.

2.4.5 Monitoring

The framework notes (p.69) that internal control systems need to be monitored. This means a process that assesses the quality of the system's performance over time. Monitoring is performed through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring includes regular management and supervisory activities and other actions personnel takes in performing their duties. The scope and frequency of separate evaluations will primarily depend on an assessment of risks and the effectiveness of ongoing monitoring procedures. According to the framework, internal control deficiencies should be reported upstream and serious matters should be reported to top management and the board.

Internal control systems are under a constant change. The way that internal controls are used may change. Efficient activities in a one point of time may become less efficient or they may no longer be performed. This can result from the arrival of new personnel, the varying effectiveness of training or supervision, time and resource constraints, or additional pressures. Also economic, operational, industry, and regulatory conditions, in which the internal control system is established in a one point of time, may have changed. As a result, internal control processes may not be able to warn about new risks. Therefore, management has to decide whether the internal control system still is appropriate and capable of indicating new risks.

Monitoring is accomplished through ongoing monitoring activities and separate evaluations. The greater scope and efficiency of ongoing monitoring activities is, the less separate evaluations are needed. Ongoing monitoring activities include e.g. management and supervision activities, comparisons, reconciliations, and other routine tasks. Separate evaluations can be directed to an individual control activity or to the entire internal control system. The latter evaluation can be done in an situation where there have been significant changes in a strategy or management, or a broad implementation or acquisition has been made.

The extent of documentation of a company's internal control system varies depending on the company's size and complexity (p.73). Larger organisations have usually written policy manuals, formal organisation charts, written job descriptions, operating instructions, and information system flow charts. Smaller companies typically have less documentation. Although internal control would not be documented, it does not mean that the internal control system would not be efficient or it could not be assessed. An appropriate level of documentation often makes assessment more useful because it helps personnel understand how the system works and what are their particular roles. It also makes it easier to modify the internal control system when necessary.

The framework states (p.74) that internal control deficiencies that can affect the company attaining its objectives should be reported to those who can take necessary actions. Deficiencies in a company's internal control system may come out from many sources, including the company's ongoing monitoring activities and separate evaluations. According to the framework, *"a deficiency may represent a perceived, potential or real shortcoming, or an opportunity to strengthen the internal control system to provide a greater likelihood that the* *entity's objectives will be achieved."* Information generated by employees in performing their operating activities is reported to their immediate superior who in turn should communicate the deficiency upstream. COSO emphasises (p.75) that findings of internal control deficiencies should not be reported only to the individual responsible for the function or activity involved, but also to at least one level of management above the directly responsible person.

2.4.6 Roles and Responsibilities

The framework states (p.83) that everyone in an organisation has some responsibility for internal control. However, management is responsible for a company's internal control system. The chief executive officer is ultimately responsible for internal control and he or she should assume the ownership of the control system. CEO sets 'tone at the top' within the organisation that affects integrity and ethical values. In a large company, the chief executive fulfils this duty by providing leadership and direction to senior managers and reviewing the way they are controlling the business. Senior managers are responsible for the establishment of more specific internal control policies and procedures to personnel who have a responsibility of the unit's functions. In a smaller company, the chief executive often is an owner-manager and therefore, the influence of the CEO is more direct. In cascading responsibility a manager is a chief executive of his or her responsibility area. Particularly significant are financial officers and their staff whose control activities cut across, as well as up and down, the operating and other units of an entity.

Management is accountable to the board of directors which provides governance, guidance and oversight. Effective board members are objective, capable, and inquisitive and they have knowledge of the company's activities and environment. Management may be in a position to override internal controls and ignore communication from subordinates enabling a dishonest management, which intentionally misrepresents results to cover its tracks. A strong and active board with effective upward communications channels and capable financial, legal, and internal audit functions, is the best authority to identify and correct such a problem.

Internal auditors play an important role because they directly examine internal controls and recommend improvements (p.88). Internal auditors evaluate the adequacy and effectiveness of the organisation's internal control systems. As COSO notes, internal control is, to some degree, the responsibility of everyone in an entity. All employees produce information used in the internal control system or take actions needed to ensure that controls are in place. All personnel should be responsible for communicating upward problems in operations, non-compliance with the code of conduct, or other policy violations or illegal actions. Because of this, internal control should be an explicit or implicit part of everyone's job description. The framework summarises (p.89) that internal control is everyone's business, and roles and responsibilities of the whole personnel should be well defined and effectively communicated.

External parties often contribute to achievement of the company's objectives (p.89). According to the framework, external auditors as the independent certified public accountants bring to management and the board of directors an independent and objective view, and contribute to a company's achievement of its financial reporting objectives, and other objectives as well. Other parties, such as legislators and regulators, customers and vendors, news and media, also provide useful information about the company's internal control. These parties, however, are not responsible for the company's internal control system.

2.5 SUMMARY

To sum up, internal control means different things to different people and therefore, there has been a confusion about the exact meaning of internal control. The literature review indicates that the goal of internal control is to ensure that the company's operations are effective and efficient, financial reporting is reliable, assets are safeguarded and, the company complies with laws and regulations. In fact, an effective control system is a precondition to both a true and fair view in financial reporting and safeguarding of organisational resources from different kinds of losses. There should also be appropriate controls in place to ensure effective and efficient operations.

Internal control is considered to be a part of a company's corporate governance. Corporate governance includes the board of directors and its committees, management, internal and external auditing, and external parties. As it was discussed in the literature review, internal control is closely related to these key components. Management and the board are responsible for organising and maintaining the company's internal control system. In practise, controlling and monitoring of a company's activities are performed as an ongoing process at all levels of organisation. Internal auditors' responsibility is to assess the adequacy and efficiency of a company's internal control system and recommend improvements. External parties, such as auditors, creditors, authorities, and customers are not responsible for a company's internal control but they contribute to the achievement of company's objectives.

To summarise, both management accounting literature and the three well-known frameworks of internal control – COSO, CoCo, and the Code of Best Practice – emphasise that internal control is to ensure that a company achieves its objectives. There can be no control without objectives and plans because these specify the desirable behaviour and set out the procedures that should be followed by the organisation in order to ensure that a company is operating in a desired manner. While management accounting literature concentrates on financial controls and management decision making, the three frameworks take a more broader view discussing issues such as integrity and ethical values, competence and skill, management's philosophy and operating style, effective and efficient operations, reliable financial reporting, compliance with laws and regulation, communication and information.

It was discussed in management accounting literature that an internal control system consists of methods and procedures to both prevent and detect errors and irregularities and to promote operating efficiency. Management control systems include administrative controls and accounting controls. These controls are mostly similar to the controls described in the COSO framework. The framework lists control activities such as approvals, authorisations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties. COSO divides controls into three categories: operations, financial reporting and compliance. These categories are, to some degree, discussed also in management accounting literature although they concentrate mostly on financial objectives.

The COSO framework is considered a common reference point. To sum up the definition of the framework, internal control is a process, which is effected by a company's board of directors, management and other personnel, and it is designed to provide reasonable assurance regarding the achievement of objectives in the following three categories: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. An internal control system is intertwined with the organisation's operating activities and exists for fundamental business reasons. Therefore, internal control is most effective when controls are built to the organisation's infrastructure and are a part of the essence of the company. "Built in" controls support quality, avoid unnecessary costs and enable quick response to changing conditions. COSO breaks down internal control into five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring. These components are derived from the way management runs a business, and are integrated with the management process. The components cut across the whole organisation and apply to all objectives categories. Determining whether a certain internal control system is effective needs an assessment of whether the five components of internal control are present and functioning effectively.

3 REGULATIVE FRAMEWORK

As a result of the 1973-1976 Watergate investigations, legislative and regulatory bodies began to give significant attention to internal control. The SEC revealed that a number of major U.S. corporations had been making illegal domestic political contributions and questionable payments, including bribes, to foreign government officials (Internal Control – Integrated Framework, p.94). In response, the Securities Exchange Act of 1934 was amended by the Foreign Corrupt Practices Act of 1977 (FCPA). Although corporate governance and internal control had been under discussion in practice for several decades, the role of internal control in detecting and preventing fraud was recognised for the first time in the federal legislation through the FCPA in the U.S. (Report of the National Commission on Fraudulent Financial Reporting 1987, p. 33). The FCPA required to establish and maintain an adequate system of internal accounting controls to provide reasonable assurance that (1) transaction are executed in accordance with management directions, (2) transactions are recorded in a manner that permits the company to prepare its financial statements according to generally accepted accounting principles or other applicable criteria and to maintain accountability for its assets, (3) access to assets is permitted only by management's authorisation, and (4) existing assets are compared with the recorded accountability of assets and action is taken with respect to differences.

In the 1980s, several commissions published their reports, which identified factors that may lead to fraudulent financial reporting. These reports gave recommendations on corporate governance, clarified the definition of internal control and instructed how to implement and assess internal control systems. Numerous associations and authorities published their recommendations on good corporate governance. In fact, there are approximately forty codes of corporate governance relevant to the EU that have been adopted over the last decade at national or international level (the European Commission's communication 2003b, p. 10). Considering the purpose of this study, the following reports published prior to the S-O act are considered important: (1) *Report of the National Commission on Fraudulent Financial Reporting* (Treadway), (2) *Code of Best Practice*, (3) *EU Green Paper*, (4) *Recommendations in Finland* and (5) *The OECD Principles.*

However, the fact was that these reports on corporate governance and internal control could only give recommendations and guidance. As a result, they just gave advices but did not have an authority to force companies. The Sarbanes-Oxley Act of 2002 was the first initiative that forced companies to organise and maintain effective internal control by legislation.

3.1 TREADWAY COMMISSION 1985

The National Commission on Fraudulent Financial Reporting, referred to as the Treadway Commission after its chairman, was established in 1985. It was a private-sector initiative, jointly sponsored by five association called as the COSO: the American Institute of Certified Public Accountants (AICPA), the American Accounting Association (AAA), the Financial Executives Institute (FEI), the Institute of Internal Auditors (IIA), and the National Association of Accountants[5] (NAA). The Commission's mission was to identify causal factors, which could lead to fraudulent financial reporting, and to create steps to reduce its incidence. The commission studied the financial reporting system in the United States and published a report with findings, conclusions, and recommendations in 1987. (Report of the National Commission on Fraudulent Financial Reporting. October 1987, p. 1)

The commission's report identifies five situations as opportunities for fraudulent financial reporting (p. 24). The first, second, and fifth relate to internal controls:

1. the absence of a board of directors or audit committee that vigilantly oversees the financial reporting process;
2. weak or nonexistent internal accounting controls (this situation can occur e.g. when a company's revenue system is overloaded from a rapid expansion of sales, an acquisition of a new division, or the entry into a new, unfamiliar line of business);
3. unusual or complex transactions (consolidation of two companies, a divestiture or the closing of specific operations, agreements to buy or sell government securities under a repurchase agreement etc.);
4. accounting estimates require significant subjective management's judgment (reserves for loan losses, the yearly provision for warranty expense etc.); and

[5] Currently called as the Institute of Management Accountants

5. ineffective internal audit staffs because of e.g. inadequate staff size or severely limited audit scope.

The commission addresses the problem of fraudulent financial reporting at two levels (p. 31). First, it recommends that top management should establish an appropriate tone, the overall control environment in which financial reporting occurs. Secondly, top management should maximize the effectiveness of functions within the company that are critical to the integrity of financial reporting. These functions include accounting and internal audit function, and audit committee. The commission emphasises that the improvement of corporate environment and culture is very important and considers 'a tone at the top' significantly affects other components of a company's control system.

Tone at the Top

The commission presents three recommendations regarding an appropriate tone at the top. According to the commission, the tone set by top management, including management philosophy and operating style, organisational structure, methods of communicating, and personnel management, is the most important factor contributing to the integrity of the financial reporting process. The commission recommends (p. 33) " *the top management of a public company to discharge its obligation to oversee the financial reporting process, it must identify, understand, and assess the factors that may cause the company's financial statements to be fraudulently misstated*". Assessment enables an entity to design and implement internal controls to minimise identified risks.

The commission also recommends that public companies should maintain internal controls that provide reasonable assurance that fraudulent financial reporting will be prevented or subject to early detection. According to the commission, accounting controls include a company's accounting system and specific control procedures. The former covers methods and records that a company uses to identify, assemble, classify, and record its transactions and the latter includes a company's individual policies for processing transactions. The commission reminds (p. 34) that internal accounting controls also include the audit committee and internal audit function. These control elements together with corporate control environment comprise the internal controls that can prevent or detect fraudulent financial reporting.

Third, the commission recommends (p. 35) that the public companies should develop and enforce the written codes of corporate conduct to create strong ethical climate. It further states that as a part of its ongoing oversight of the effectiveness of internal controls, a company's audit committee should review annually the program that management establishes to monitor compliance with the code. The code's effectiveness is mostly determined by the attitude and behaviour of a company's top officers and directors, who should act as an example for the entire company.

Accounting and Internal Audit Functions

The commission recommends (p. 36) that public companies should maintain accounting functions that are designed to meet their financial reporting obligations. It highlights that as a member of top management, chief finance officer helps set the tune of the organisation's ethical conduct. The CFO is part of the control environment and is generally responsible for designing, implementing and monitoring the financial reporting system and the internal accounting controls.

The commission also gives recommendations regarding internal audit function by stating that public companies should maintain an effective internal audit function with an adequate number of qualified personnel appropriate to the size and the nature of the company (p.37). Further, it emphasises that the internal audit function has to be objective and independent and that the chief internal auditor should have a high status within the organisation.

Management's Reporting

Users of financial statements should be better informed about the roles management play in the company's financial reporting process. The commission recommends (p. 44) that all public companies should be required by a SEC rule to include a management report in their annual statements that "*acknowledges management's responsibility for the financial statements and internal control, discussses how these responsibilities were fulfilled, and provides management's assessment* of *the effectiveness of the company's internal controls.*" It is interesting to notice that Section 404 of the Sarbanes-Oxley Act of 2002 enacted these recommendations about fifteen years later by requiring a company's managers to state their responsibility on internal control, clarify methods used in the internal control processes and assess the effectiveness of internal control. On the other hand, Treadway commission and its sponsors were the authors of the COSO framework, which has been used as a reference point in the S-O act.

Finally, the commission recommends (p. 48) that its sponsoring organisations should cooperate in developing additional, integrated guidance on internal controls. They should work together to integrate the various internal control concepts and definitions and to develop a common reference point. This would help public companies to judge the effectiveness of their internal controls, and improve their internal control system. In response, the COSO organisation undertook an extensive study of internal control to establish a common definition, which would serve the needs of companies, independent public accountants, legislators and regulatory agencies. In 1992, COSO provided a broad framework of internal control, which has already been discussed in this study.

3.2 CADBURY COMMITTEE 1992

A continuing concern about the quality of financial reporting and accountability along with the business scandals, such as BCCI and Maxwell in the late 1980s, resulted in the establishment of the Cadbury Committee. The committee was named after its chairman Sir Adrian Cadbury and it was established by the Financial Reporting Council, the London Stock Exchange and the accountancy profession in the UK. In 1992, the committee published a report "Code of Best Practice", which included nineteen recommendations on corporate governance. These recommendations focused on internal control, reporting of the boards of directors, and the role of auditors. The committee's purpose was to review the aspects of corporate governance, which specifically related to financial reporting and accountability (para. 1.2), and to create a framework for ensuring that managers reviewed the controls in their business (para. 2.1). The code was to assist the efficient operations of capital markets and increase confidence in boards, auditors and financial reporting (para. 3.5).

The principles of the code are openness, integrity and accountability. Openness is a basis for confidence, which needs to exist. Open approach to the disclosure of information enables boards to take effective actions and allows shareholders and other parties to look into companies in detail (para. 3.2). Integrity means straightforward dealing and completeness. These are required to present a true and fair view in financial reporting. The integrity of reports depends on the integrity of individuals preparing and presenting them (para. 3.3).

The committee emphasises that all employees must know what kind of standard of conduct is expected of them. It recommends that the boards of directors should establish codes of ethics or statement of business practice and publish them both internally and externally. (para. 4.29)

Directors are responsible under s.221 of the Companies Act 1985 for maintaining adequate accounting records. To meet these responsibilities management needs to maintain the internal control system over the financial management, including procedures to minimise the risk of fraud. Therefore, there already is an implicit requirement on directors to ensure that a proper system of internal control is in place (para. 4.31). An effective internal control system is a key element of a company's efficient management. The Cadbury's code also recommends that *"the directors should make a statement of their internal control system and that they should assess the effectiveness of internal control"*.(para. 4.32)

The committee recommends that an audit committee should review the company's statement on internal control system prior to endorsement by the board (para. 4.35(v)). According to the committee, companies should establish internal audit functions to undertake regular monitoring of key controls and procedures. The Committee states that such regular monitoring is an integral part of a company's internal control system and helps ensure its effectiveness. It highlights that internal audit should have a direct access to the chairman of the audit committee to ensure the independence of their position. (para. 4.39)

The committee recommends that auditors should report on management's statement of their internal control system (para. 4.32). This recommendation became mandatory for the external auditors of American public companies when the S-O act regulated that a company's auditors have to issue an attestation report. Similarly to Treadway commission, Cadbury report also recommended that the accountancy profession and representatives of preparers of accounts should take the lead in developing a set of criteria for assessing effectiveness, guidance for companies on the form in which managers should report, and also guidance for auditors on relevant audit procedures and the form in which auditors should report (para. 5.16).

Both Treadway and Cadbury committees state that an organisation should be established that would develop internal control concept and criteria. To sum up, both of these committees clearly state that a company's management should assess the effectiveness of internal control. Yet, many questions remain open and neither of the committees give clear advices on the following questions: What kind of statement should management give on the company's internal controls? How is the effectiveness of internal control assessed and measured? How is the regular monitoring of key controls arranged in practice? By that time, there were a lot of requirements relating to public companies' internal control system but none of the reports gave concrete instructions on how to develop effective internal control processes in practice. Because of this, it is not a surprise that both Treadway and Cadbury committees promoted that integrated guidance on internal controls should be developed.

3.3 EU GREEN PAPER 1996 AND SUBSEQUENT COMMUNICATIONS

Internal control systems and reporting on those systems are not included in any European Directive on accounting or auditing. However, European Commission took first major steps when a Green Paper was published in 1996, titled as "*The Role, the Position, and the liability of the Statutory Auditor within the European Union*" (Maijoor, 2000). The Green Paper provided recommendations on auditing and internal control. It suggests an auditor's attest on internal control systems and this attestation should be included in the audit report. The Green Paper also notes that there should be a strong internal audit function within organisation. It states that external auditing is not sufficient and it should be supported by the internal audit activities, which are carried out on a continuing basis.

The increasingly more important role of internal control can also be noted in the European Commission's communication on the statutory audit in the European Union (1998, p. 4). The communication states that companies should pay more attention to internal control, internal audit and risk management. The reorientation of the EU policy on statutory audit – urged by recent financial scandals – continued with Commission's communication on *"Reinforcing the statutory audit in the EU"* in 2003. This communication includes actions relating to corporate governance, audit committees, and internal control and states that the quality of a company's internal control system is an important issue. The Commission adds that several corporate governance codes are used in the EU and some laws in the Member States require statutory auditors to specifically report on the internal control system. The Commission proposes that present situation in the EU on the statutory auditor's involvement in the assessment and reporting on internal control systems will be examined and the need for further initiatives will be identified. The suggested timeframe for this examination is 2004-2006 (2003a, p. 19-20).

The parallel communication *"Modernising Company Law and Enhancing Corporate Governance in the European Union - A Plan to Move Forward"* was published in May 2003. It states that a company law and good corporate governance practices throughout the EU will enhance the efficiency and competitiveness of business and strengthen shareholders rights and third parties protection. The most interesting statement (2003b, p.5) relates to developing of regulation relating to corporate governance: *"the EU must define its own European corporate governance approach... Corporate governance is an area where standards are being set at international level..."* The communication refers to the Sarbanes-Oxley Act of 2002 and points out that the EU shares the same objectives and principles in many areas as the S-O act .

The communication concludes that based on the review of main corporate governance codes the EU should not devote time and effort to the development of a European corporate governance code (2003b, p. 11). However, it suggests that a common approach should be adopted at EU level with a few essential rules and that adequate coordination of corporate governance codes should be ensured. The communication summarises that the approach would guarantee of the best governance practices and that non-binding rules are not always sufficient (2003b, p. 12).

3.4 RECOMMENDATIONS ON INTERNAL CONTROL IN FINLAND

In 1997, a report "Corporate Governance Recommendations for Listed Companies" was published in Finland by the following parties: Helsinki Stock Exchange, the Central Chamber of Commerce in Finland and the Confederation of Finnish Industry and Employers. A working group, set by the parties, examined relevant Finnish legislation and regulation. The following legislation was considered significant: The Finnish Companies Act (OYL), the Securities Markets Act (AML) and the Auditing Act (TTL). Essential authority regulation included the decisions of the Ministry of Finance by the Securities Markets Act. Helsinki Stock Exchange rules and the recommendations on generally accepted auditing standards developed by the Finnish Institute of Authorised Auditors was considered as relevant self-regulation.

The report covers mostly issues relating to companies' boards of directors and states only one recommendation on internal controls. The report recommends that to take care of business efficiently and compliance with laws, sufficient control activities should be organised (p. 35). It points out that internal control systems, which include procedures, control activities, and regular reporting, vary a lot depending on a company's operations and size. The working group summarises that the chief executive officer is responsible for organising a company's internal audit because the CEO is also responsible for the compliance of company's accounting practices with law in day-to-day operations and reliable financial reporting.

The report states that the organisation and working methods of internal audit depend on a company's business, the amount of employees, training and technical systems used in the operations (p.36). Resulting from this diversity of public companies, they do not give a general recommendation on the organisation of internal audit (p.37). In addition, the report does not recommend companies to establish an audit committee, but leaves this decision for the companies. Finally, the report recommends that there should be an active internal control system, which ensures the appropriate organisation of a company's accounting, safeguards assets and other central activities. Public companies should define the principles of internal controls and procedures that ensure the effectiveness of internal control system. Particular attention should be given to organising of control activities, directives and internal audit (p. 39).

There are a couple of interesting points in the report. First, the recommendations on internal control system handle mostly *internal audit*. This may result from the fact that public discussion on internal control from a management's point of view was not comprehensive at that time. There was no internal control guidance published in Finland. Secondly, the report does not define the concept of internal control. It does not clarify of which components the internal control system consists and it gives mostly recommendations on managers' responsibilities. It seems that the concept of internal control was not very clear.

In 2003, these recommendations for Finnish listed companies were reviewed by a working group appointed by the same parties. The objective of these updated recommendations was *"to harmonise the practices of listed companies, improve transparency of their operations, harmonise the information given to shareholders and improve the quality of disclosure"* in order to increase local and international investors' interest in Finnish listed companies and promote trust in the securities markets. Listed companies should comply with the recommendation of 2003 starting from July, 1st 2004. The recommendations state that the reason for any deviations of the recommendations have to be explained and that companies have to give information on the compliance with the recommendation both in their annual statements and on the websites. (2003, p. 4)

Contrary to the prior report, the updated recommendations state (p. 10) that the audit committee should be established, *"if the extent of the company's business requires preparation of matters relating to financial reporting and control to be dealt with by a group with more compact composition than the entire board."* The report clarifies that the extent of a company's operations may require some directors to concentrate particularly on matters relating to financial reporting and control. The audit committee has better possibilities than the entire board to review financial administration and control of the company, and ensure contacts with auditors and the internal audit function.

The recommendations handle internal control, risk management and internal audit (2003, p. 15). The working group states that the purpose of internal control and risk management is to ensure the effective and successful operations, reliable information and compliance with the relevant regulations and operating principles. This definition is similar to the definition in the COSO framework. It further states that internal control helps improve the effective fulfilment of the board's supervising obligation. Recommendation 49 points out that the company's board of directors should define internal control procedures and ensure that the effectiveness of internal controls is regularly assessed and monitored to ensure successful operations. Recommendation 50 handles risk management and it points out that *"the company shall describe the criteria according to which the risk management is organised."* It notes that the purpose of risk management is to ensure that the risks related to the business operations of the company are identified and monitored. This definition also is similar to the COSO framework. The recommendation further points out that effective risk management requires specific guidelines and that both shareholders and the board are informed about the significant risks.

3.5 OECD PRINCIPLES OF CORPORATE GOVERNANCE 1999

In 1999, OECD published "OECD Principles of Corporate Governance". The objective of the principles is to help governments "*evaluate and improve the legal, institutional and regulatory framework for corporate governance in their countries, and provide guidance and suggestions for stock exchanges, investors, corporations, and other parties that have a role in the process of developing good corporate governance*." The focus is publicly traded companies (1999, p. 2). The OECD principles cover five areas: I The rights of shareholders, II The equitable treatment of shareholders, III The role of stakeholders, IV Disclosure and transparency, and V The responsibilities of the board. The OECD principles handle more corporate governance in general than internal control in detail. However, the principles IV and V are presented shortly because they discuss the factors relevant also to internal control. These factors are risks, companies' objectives, accountability, responsibilities, and the oversight of management.

Principle IV "Disclosure and transparency" states that the corporate governance framework must ensure timely and accurate disclosure on all material matters regarding the company. This includes the financial situation, performance, ownership and governance of the company. It says that disclosure should include e.g. company objectives, information on material foreseeable risk factors and governance structures and policies (1999, p. 8). The principle encourages to disclose policies relating to business ethics, as well as operational or financial objectives. It also recommends (p. 20) to give information on reasonable material foreseeable risks, which can include industrial or geographical risks, or risks related to off-balance sheet transactions, for instance.

Principle V "The responsibilities of the board" states that the corporate governance framework must ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders. This includes that the board should ensure compliance with applicable laws and regulation and fulfil the following key functions (1999, p. 9): (1) reviewing and guiding corporate strategy, major plans of action, risk policy, setting performance objectives, monitoring implementation and corporate performance; (2) ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for monitoring risks, financial control, and compliance with the law; (3) monitoring the effectiveness of the governance practices under which it operates; and (4) overseeing the process of disclosure and communications.

The principles do not specifically provide guidance on the internal control. However, the principles discuss on some elements of internal control and expect companies to organise control activities and provide internal control guidelines. These include e.g. determining the objectives of the company, defining policies and business ethics, assessing material risk factors, and monitoring the compliance with applicable laws.

3.6 THE SARBANES-OXLEY ACT OF 2002

3.6.1 Background and Objectives

On July 30th 2002, President Bush signed a law called as the Sarbanes-Oxley Act of 2002 (H.R. 3763). The act is to strengthen corporate governance and restore trust in the public securities market. The act was sponsored by US Senator Paul Sarbanes and US Representative Michael Oxley and it was passed in response to a number of major corporate and accounting scandals involving well-known corporations in the United States, such as Enron and WorldCom. These scandals along with other financial scandals throughout history of several decades resulted that the US authorities decided corporate governance recommendations and regulations not to be sufficient to ensure a true and fair financial reporting, but it had to be forced by legislation.

The government enacted the S-O act *"to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws"* (Sarbanes-Oxley Act of 2002, p. 1). The act is intended to improve corporate governance, promote ethical business practices and enhance the transparency of financial statements and disclosures. It is also intended to ensure that company executives are aware of material information threatening their business, and hold management accountable for material information filed with the SEC and released to investors (McNally 2004, p.1).

3.6.2 Scope and Definitions

The S-O act contains eleven titled sections and nearly 70 subsections (Appendix 1). It establishes new standards for the board of directors and audit committees, accountability standards and criminal penalties for top management. In addition, it establishes new standards relating to external auditor's independence and the Public Company Accounting Oversight Board (PCAOB, supervised by the SEC), which is to oversee public accounting firms and issue accounting standards.

Section 3 (a) of the S-O act "Commission Rules and Enforcement" defines the regulatory action: *"The Commission*[6] *shall promulgate such rules and regulations, as may be necessary or appropriate in the public interest or for the protection of investors, and in furtherance of this Act."* The act authorises the SEC to announce the final rules. Section 3 (b)(1) regulates the enforcement in general by saying that:

> *"A violation by any person of this Act, any rule or regulation of the Commission issued under this Act, or any rule of the Board shall be treated for all purposes in the same manner as a violation of the Securities Exchange Act of 1934 or the rules and regulations issued thereunder, consistent with the provisions of this Act, and any such person shall be subject to the same penalties, and to the same extent, as for a violation of that Act or such rules or regulations."*

---

[6] The term "Commission" in the act means the Securities and Exchange Commission (SEC)

The act applies to the companies whose shares are listed in a securities exchange registered with the SEC.[7] There are several effective dates of the S-O Act. The *original* compliance dates of section 404 are set by the SEC and apply to the companies other than registered investment companies. An American public company having more than $75 million in market capitalisation – called as "accelerator filer" in the SEC ruling – will have to comply with the law in 2004, if their fiscal year ends on or after June 15, 2004. Smaller and foreign private companies, called as "non-accelerator filers", must begin to comply with the requirements for its fiscal year ending on or after April 15, 2005 (SEC Final Rules 2003, Release No. 33-8238).

The law and, particularly, section 404 set enormous requirements for the companies, which are facing a variety of problems when making efforts to comply with the law. Because of this, the SEC extended the compliance date so that the accelerator filers must begin to comply with the management report on internal control over financial reporting disclosure requirements for its fiscal year ending on or after November 15, 2004 (SEC Final Rules 2004, Release No. 33-8392). The compliance date for non-accelerator filers have also been extended. In the last extension on March 2nd 2005, the SEC announced that non-accelerator filers have to comply the requirements on or after June 15, 2006 (SEC Final Rules 2005, Release No. 33-8545). The reason for this additional relief is problems faced by foreign companies with language, culture and organisation structures that are different from what is typical in the US. However, the most important reason is that the SEC admits that companies, which are publicly traded within the EU, are required to prepare their consolidated financial statements under IFRS and they have to focus on those requirements.

3.6.3 Section 404: Management Assessment of Internal Controls

---

[7] Currently, there are nine securities exchanges registered with the SEC. These are: American Stock Exchange, Boston Stock Exchange, Chicago Board Options Exchange, Chicago Stock Exchange, International Securities Exchange, National Stock Exchange (formerly the Cincinnati Stock Exchange), New York Stock Exchange, Pacific Exchange, Philadelphia Stock Exchange. Note that the Nasdaq Stock Market is not a registered national securities exchange. (http://www.sec.gov/divisions/marketreg/mrexchanges.shtml. 10.3.2005)

It is interesting to notice that there is a lot of text pressed in the act regarding PCAOB, auditor independence and corporate responsibility but only limited focus with six sentences on section 404 "Management Assessment of Internal Controls". However, compliance with this section may, ironically, cause most difficult and costly challenges. It may result in additions of dedicating staff, investments in software or third-party consultants to document, assess and test a company's internal controls, and increasing external audit fees due to an auditor's new responsibilities, for example.

The content of the section 404 (a) is and rules required are as follows. "The Commission shall prescribe rules requiring *each annual report ... to contain an internal control report*, which shall:

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year, of the effectiveness of the internal control structure and procedures for financial reporting."

Next, S404 (b) legislates that *"with respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board8. Any such attestation shall not be the subject of a separate engagement."*

3.6.4 SEC Final Rule

SEC adopted the Final Rules on management's reports on internal control over financial reporting in May, 2003. The rule specifies the requirements set to the management's report on internal control over financial reporting. First of all, SEC states that a company should design a process supervised by the board of directors, management and other personnel to provide

[8] The term "Board" means the PCAOB established under section 101.

reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements in accordance with generally accepted accounting principles. The process should include those policies and procedures:

- pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the company;
- provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of a company are being made only in accordance with authorisations of management and directors;
- provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements

Secondly, the final rule handles management's annual assessment of company's internal control over financial reporting and management's report thereon. It requires a company's annual report to include an internal control report of management that contains:

a) a statement of ***management's responsibility*** for establishing and maintaining adequate internal control over financial reporting for the company;

b) a statement ***identifying the framework*** used by management in the evaluation of the effectiveness of the company's internal control over financial reporting;

c) ***management's assessment*** of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year;

d) a statement that the registered public accounting firm has issued ***an attestation report*** on management's assessment of internal control over financial reporting.

Management's assessment must include a statement as to whether or not the company's internal control over financial reporting is effective.[9] The assessment must also include disclosure of any *"material weaknesses"*[10] in the company's internal control over financial reporting identified by management. SEC states that management is not permitted to conclude that the company's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting. In addition, auditor's attestation (404 b) cannot be the subject of a separate engagement of the registered public accounting firm. It is also required that a company files the attestation report of the registered public accounting firm that audited the company's financial statements as part of the company's annual report.

Third, SEC final rule discusses the requirement of the evaluation criteria. It specifies that management must base its evaluation of the effectiveness of the company's internal control over the financial reporting *"on a suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment."* However, it notes that the COSO framework meets the requirements of SEC but also other frameworks, as CoCo and Turnbull, can be used.

Next, the rule discusses the cooperation between auditors and a company's management. It states that because auditors have to issue an attestation report, management and the company's independent auditors will need to coordinate their processes of documenting and testing the internal controls over financial reporting. The auditors may assist management in documenting internal controls. When the auditor is engaged to assist management in documenting internal controls, management must be actively involved in the process. The rule reminds that management cannot delegate its responsibility to assess its internal controls over financial reporting to the auditor.

---

[9] A negative assurance statement indicating that nothing has come to management's attention to suggest that the company's internal control over financial reporting is not effective will not be acceptable.

[10] "Material weakness" can be described as "significant deficiency". Both represent deficiencies in the design or operation of internal control that could affect a company's ability to record, process, summarise and report financial data consistent with the assertions of management in the company's financial statements.

The method or procedures to be performed in the evaluation process are not specified in the final rule. However, the rule states that the assessment must be based on procedures, which are sufficient both to evaluate the design of a control and to test the operating effectiveness of this control. For example, controls subject to such assessment can be: (1) controls over initiating, recording, processing and reconciling account balances; (2) controls related to the initiation and processing of non-routine and non-systematic transactions; (3) controls related to the selection and application of appropriate accounting policies; and (4) controls related to the prevention, identification, and detection of fraud.

The rule further states that the assessment of the effectiveness of internal control over financial reporting must be supported by evidential matter, which includes documentation on both the design of internal controls and the testing processes. This evidential matter should provide reasonable support for the evaluation of whether the control is designed to prevent or detect material misstatements or omissions. It should also provide reasonable support for the conclusion that the tests were appropriately planned and performed and that the results of the tests were appropriately considered. In addition, it is stated that the public accounting firm (that attests) will require the company to develop and to maintain such evidential matter to support management's assessment. Finally, the final rule discusses the location of management's report in the annual statement. It does not specify where the report should be placed but recommends that it should be in close proximity to the corresponding attestation report issued be the company's registered public accounting firm.

3.6.5 Implementing S404: A Practical Approach

Quall (2004) presents a five-step methodology, which may help companies implement section 404. Exhibit 2 presents the five different steps. First, Quall recommends companies to form a sponsoring committee, a project team, and a formal written plan. He highlights that a successful internal control project requires an ongoing support of senior management and the board of directors. Senior management should truly believe that implementing section 404 increases the value of company in the long run and it is not just a legal obligation. Senior management sets the tone at the top and it should also ensure that necessary resources are available to the project. Quall notes that it is essential to make a written plan, which includes a clear statement about the requirements, a timeline with obtainable milestones, and a realistic estimate of required resources. Also communication with outside professionals, such as auditors and legal counsel, is important.

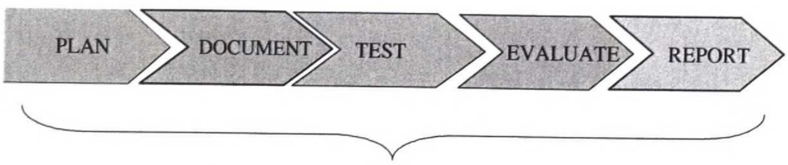


Figure 2: Quall's five-step methodology

The second step is to document the financial cycles. As Quall points out, all public companies already have internal control structure but it may not be formally documented. Documenting internal control includes three common methods: narratives, flowcharts and internal control questionnaires. These can be used separately or in combination. Documentation should be traced back to the company's policies and procedures. Quall clarifies that a narrative is a written description of a company's internal controls and financial cycles. It should describe every document and record used in the accounting system and every process that occurs, whether manual or computer-generated, drilled down to the lowest level possible. The narrative should also indicate the identified controls, e.g. authorisations, approvals, and separation of duties, related to the document or procedure. A flowchart in turn is a symbolic presentation of a company's flow of documents and processes.

Third, Quall recommends that transactions should be tested to verify that identified internal controls are performing as they were designed to do. The test of transactions should be made in two directions: "cradle-to-grave" and "grave-to-cradle". The former means that a sample should be made of certain source documents, e.g. vendor invoice or sales transaction, and two questions should be addressed: 1. Do internal controls handle the transactions in the matter designed? 2. Do all transactions reach the financial statements? The latter traces a sampling of transactions from a financial statement back to the source document. A test in this direction addresses the issue of whether all data contained in a financial account balance is supported by a source documentation.

Quall notes that the sample of transactions tested in both directions should be selected using a sampling technique, which can be either a judgemental or statistical. A judgemental approach is a systematic selection of days of the fiscal year or every 100^{th} transaction in a numerical sequence, where as a statistical approach would take a random sample from all transactions. Quall refers to the Statement on Auditing Standards (SAS) No 31, "Evidential Matter", by stating that the tests of transactions should be designed to test management assertions. SAS 31 classifies these assertions into five categories:

Existence or occurrence – Assets, liabilities and equity actually exist on the balance sheet date and that recorded transactions included in the financial statements actually occurred during the period (e.g. inventory that exist and is available for sale at the balance sheet date).

Completeness – The financial statements include all transactions and accounts that should be presented (e.g. sales cut-off test).

Valuation and allocation – Asset, liability, equity, revenue, and expense accounts have been included in the financial statement at appropriate values (e.g. fixed assets stated at the net book value).

Rights and obligations – The assets are the rights of the company and the liabilities are the obligations of the company at the balance sheet date.

Presentation and disclosure – Components of the financial statements are properly classified, grouped, and disclosed in the financial statements (e.g. liabilities properly recorded as a current or long-term liability).

The fourth step is to evaluate the test results. The documentation of evaluation should describe the procedures used and the results obtained about operating effectiveness to provide a basis for conclusion. If a tester identifies internal control deficiencies during the evaluation, plans to remedy these internal controls should be documented and implemented. A corrective action should be taken as soon as possible. Quall notes that the corrected internal control procedure must be in place for a period of time prior to the reporting date so that management is able to evaluate the corrected control and conclude that the control is effective as of the reporting date.

Internal control deficiencies are classified into two categories. The first category is *significant deficiencies*, which means an internal control deficiency that could adversely affect the company's ability to record, process, and report financial data consistent with the assertions of management in the financial statements. The second category is *material weaknesses.* A material weakness is a reportable condition, which is so serious that one or more internal control elements do not reduce to a relatively low level the risk that material misstatements in the financial statements will not be prevented or detected on a timely basis. The presence of a material weakness may indicate that the internal control system is not effective.

As Quall points out, the evaluation is an ongoing process and is has to become a part of the culture. According to SEC rules, a company must report on internal control for every reporting period. The evaluation has to be extensive but the collection of data does not have to be as extensive as the initial implementation. He also notes that companies have to update the internal control process *on a quarterly basis,* and fully evaluate it annually.

The last step in Quall's methodology is to report. The SEC final rule states that a company's annual Form 10-K must report management's responsibilities to establish and maintain adequate internal controls for the company. The SEC final rule sets certain requirements for the content of this management report. These requirements have already been discussed in detail.

3.6.6 Challenges and Benefits

According to the S-O act, there has to be evidential support regarding a company's internal control system. The requirement of extensive supporting documentation may become a challenge for companies. Management has to prove that the company's internal controls are effective. Therefore, a company should have supporting documentation, which describes controls activities of the company and proves that the company's test plans are prepared and that testing is performed in practice. There should also exist documentation that the results of such testing were considered in the final evaluation of internal control over financial reporting. Additionally, the assessment of internal control requires the disclosure of any material weaknesses in the company's internal control system. Testing and defining key controls are time consuming and will be a challenge because individuals may not be familiar with statistical terms and testing procedures. As a result, it is likely that training of relevant people within the organisation becomes necessary.

Although companies may see the compliance of the S-O Act as a 'burden', they should also see its opportunities. As companies work to comply with these new rules, they may have an opportunity to address other aspects of risk throughout the organisation, including financial, legal, and operational. Evaluating and monitoring of business risks helps companies meet their strategic goals and focus on corporate governance at the same time (Farrell, 2004). The self-assessments of the risks and controls and a documentation of a variety of processes may help companies to understand better their activities within the organisation.

There has been conventional wisdom that the responsibility of internal controls is delegated to the finance staff in the organisation. However, according to current thinking internal controls are owned by those within the business who manage daily operations and who depend on the controls for achieving their goals (Farrell, 2004). These control process owners have the best knowledge to identify, evaluate and assess the possible risks and to assist the business in achieving its financial goals. Because of this, process owners may take a greater responsibility for controls. Assessment of internal control may lead to greater use of controls, better evaluation of process risks, more uniform controls throughout the organisation.

3.7 SUMMARY

The Foreign Corrupt Practices Act of 1977 recognised the role of internal control in detecting and preventing fraud for the first time in U.S. legislation. The FCPA required to establish and maintain an adequate system of internal accounting controls. In the 1980s, considerable attention was paid toward internal control by a number of public, private and professional bodies, which issued recommendations or requirements on internal control. These bodies included Treadway, Cadbury, COSO and OECD, for example. There was a growing interest to clarify the definition of internal control by creating common frameworks and to instruct how to maintain and assess companies' internal control systems.

The Treadway Commission had its objective to identify the causal factors of fraudulent financial reporting and to make recommendations to reduce its incidence. The commission made a number of recommendations directly concerning internal control. It emphasised the significance of control environment, codes of conduct, competent audit committees and an active and objective internal audit function. The commission also called for the sponsoring organisations to work together to integrate various internal control concepts and definitions. In response, the COSO organisation undertook an extensive study of internal control to establish a common definition, which would serve the needs of companies, independent public accountants, legislators and regulatory agencies.

In 1992, the Cadbury committee published a report "Code of Best Practice" in UK and the recommendations also focused on internal control. The principles of the code were openness, integrity and accountability, which enable management to take effective actions, allows external parties to look into companies in detail and enables a true and fair view in financial reporting. OECD published its principles on good corporate governance, in which it also discussed internal control in some extent. The principles encouraged companies to disclose policies relating to business ethics, as well as operational or financial objectives and OECD states that the company should ensure compliance with applicable laws and regulation. The principles also require that companies should ensure the integrity of the corporation's accounting and financial reporting systems and that appropriate systems of control are in place for monitoring risks and financial control.

In 2003, certain professional bodies published the corporate governance recommendation for listed companies in Finland. These recommendations also handle internal control, risk management and internal audit and they state that the purpose of internal control and risk management is to ensure the effective and successful operations, reliable information and compliance with the relevant regulations and operating principles. This definition was similar to the objectives of internal controls described in the COSO framework.

The Sarbanes-Oxley Act was enacted in US in 2002 in response to a number of major corporate and accounting scandals. This was the first time that internal control requirements were forced by the law. The S-O act is to improve corporate governance, promote ethical business practices and enhance the transparency of financial statements and disclosures. Section 404 concentrates on management assessment of internal control. The SEC final rules give a real picture of the scope of section 404. Although public companies are required by the security exchanges or authorities to comply with the recommendations, there has never been such an extensive requirement for establishing the internal control system. The SEC-reporting companies have to assess the effectiveness of the internal control structure and procedures for financial reporting. The management have to state their responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting. In addition, external auditors of the company have to attest to, and report on, the assessment made by the management in the auditor's report.

4 PRIOR RESEARCH

The literature review of this study discussed that there has been a confusion in practice about the definition of internal control over the decades. According to Maijoor (2000), this confusion also applies to internal control *research.* Internal control is studied in various areas of accounting research, covering very different concepts, and studying controls at different organisational levels. He argues that internal control is not yet a separate category of research and that the research on internal control is not addressing issues relevant to the public policy debates on internal control, auditing, and corporate governance. In this study, the following areas are covered in presenting prior empirical researches: definition of internal control, demand for internal control system and demand for reporting on internal control. In fact, the S-O act S404 already covers all these areas. However, it is important to examine what has been stated about these issues prior to the act.

4.1 DEFINITION OF INTERNAL CONTROL

The concept of internal control can be determined narrowly covering only financial controls or a broader view can be taken as in the COSO and CoCo frameworks. According to Maijoor (2000), there are three areas of internal control research in the academic accounting literature. These are (1) internal control from an auditing perspective, (2) internal control from an organisation theory perspective, and (3) internal control from an economics perspective. Internal control research from an auditing perspective concentrates on traditional accounting controls in the context of decision making by auditors. Maijoor states that the focus is mainly on the effect of accounting controls on the reliability of financial reporting and argues that e.g. the concept of control environment receives limited attention although it is a standard issue in audit manuals of international audit companies.

Maijoor (2000) claims that internal control research from an organisation theory perspective, i.e. a management control perspective, takes a broader view than auditing research. Merchant (1998) defines action controls, result controls, and personnel and cultural controls. These controls include traditional accounting controls (emphasised by auditing research), behavioural controls and controls relating to corporate culture. As Maijoor notes, the COSO framework combines these two literatures. Finally, he states that the internal control research from an economics perspective is dominated by agency theory and studies on reward systems, bonus plans, monitoring and bonding mechanisms.

Spira and Page (2003) depict the trend away from a narrow definition of internal control toward a broader scope (Figure 3). According to them, the Cadbury's report limited mainly to financial aspects, where as both COSO and CoCo cover operational controls, and compliance with laws and regulation besides financial controls. They claim that both COSO and CoCo clearly extend their definitions of internal control but defining internal control boundaries remains problematic.

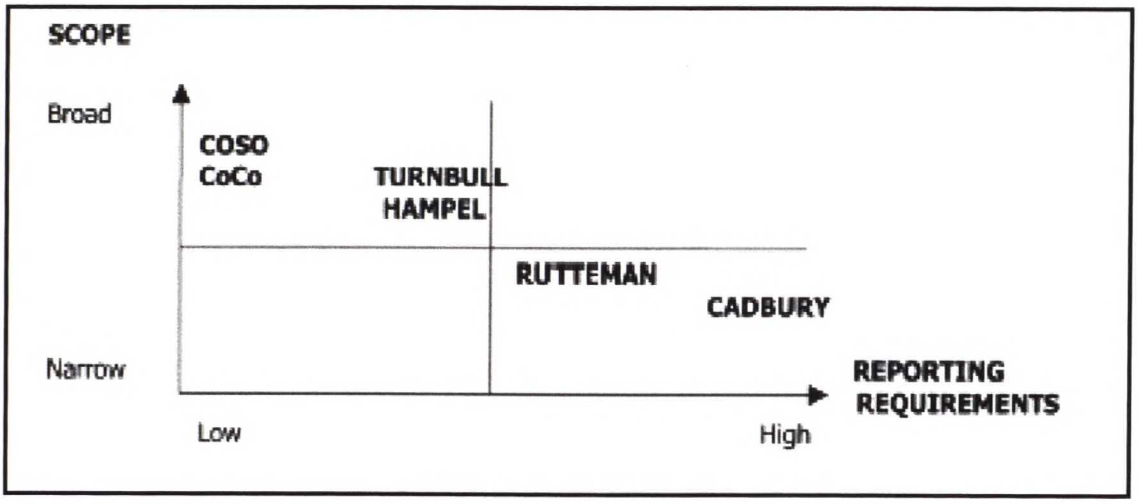


Figure 3: The trend away from a narrow definition toward a broader scope definition

4.2 DEMAND FOR INTERNAL CONTROL SYSTEM

Spira and Page (2003) identify two factors, which hastened the expansion of internal control in 1980s and 1990s: *(1) growth of information technology* and *(2) changes in audit methods.* The authors state that the technological change began when maintenance of records on real time databases became widespread. Large databases and the reduction in the cost of software for accessing and manipulating data meant that the traditional processing controls became outdated. They further explain that external auditors were under a pressure to reduce fees, and to become more "relevant to the management of their clients" because of governments' unwillingness for intervention in the late 1980s. As a result, the auditing of financial statements evolved from a process of detailed testing of transactions and account balances toward a process of samspling and testing. Therefore, auditors' considerations of a company's internal control became necessary in planning an audit. Spira and Page conclude that these changes in technology and auditing encouraged a devolution of control downwards in organisations.

Beasley et al. (1999) examined company and management characteristics of approximately 200 companies, which involved recent financial statement fraud during the years 1987-1997. They found that these companies were typically small and the most of them were not listed in the New York or American stock exchanges. The most significant result was that the companies with financial statement fraud had a poor "tone at the top" and that corporate governance activities were ineffective. As an evidence of this poor business ethics was the fact that the frauds went to the very top of the organization. In 72 percent of the cases, the CEO appeared to be associated with the fraud.

The COSO framework (p. 24) refers to Merchant's study (1987), in which he examined organisational factors that may affect the likelihood of fraudulent financial reporting. The study identified the following factors that may give individuals a strong incentive to take dishonest, illegal, or unethical actions:

- *pressure to meet unrealistic performance targets, particularly for short-term results*
- *high performance-dependent rewards*
- *upper and lower cut-offs on bonus plans*

Additionally, Merchant defined "temptations" for employees to engage in improper acts:

- *nonexistent or ineffective controls, such as poor segregation of duties in sensitive areas that offer temptations to steal or to conceal poor performance*
- *high decentralisation that leaves top management unaware of actions taken at lower organisational levels and thereby reduces the chances of getting caught*
- *a weak internal audit function that does not have the ability to detect and report improper behaviour*
- *an ineffective board of directors that does not provide objective oversight of top*

management

- *penalties for improper behaviour that are insignificant or unpublicised*

These factors may have an effect on the ethical behaviour within an organisation. Removing these incentives and temptations is likely to improve the control environment by reducing improper behaviour and therefore, the risk of unreliable reporting and misuse of company assets is likely to diminish.

4.3 DEMAND FOR REPORTING ON INTERNAL CONTROL

Several recommendations and principles – Treadway, Cadbury, OECD, SEC – and specifically, the Sarbanes-Oxley Act of 2002 assume that the reporting on the effectiveness of internal control over financial reporting will strengthen corporate governance and improve public trust in the capital markets by increasing the reliability and the transparency of financial reporting. However, there is scarce empirical evidence on the beneficial effects of reporting on internal control. Are internal control reports valued? If so, by whom and why? Are reports useful? Hermanson (2000) divides the debate of management's reporting on internal control (MRIC) in three issues as follows: 1. should it be voluntary or mandatory, 2. should auditors attest to MRICs, and 3. should the definition of control be confined to financial reporting?

Wallace (1982) surveyed various groups to assess the effects of MRICs. The sample included 64 investment officers, 13 lending officers, 13 Certified Financial Analysts, 12 directors, 12 controllers, and 18 CPAs and she found that the major part of the respondents opposed auditor reporting on internal control. Further, over a half of the respondents believed that auditors' attestation on MRICs would lead to increased audit costs, increased internal control costs to cover liability risk, incorrect assumptions by the users about the long-term adequacy of controls, and the incorrect belief that fraud is prevented. (quoted in Hermanson 2000, p. 327)

Ragahundan and Rama (1994) analysed the annual reports 1993 of Fortune 100 companies and found that 80 of the 100 companies included a management's report on internal control in their annual report. They note that although the COSO report provides a specific guidance about the issues to be addressed in such reports, the reports were still quite diverse. Ragahundan and Rama found that all 80 companies reported that they *maintain* their internal control system and *describe* the internal control system in varying levels of detail. However, only four of the 80 companies provided information required by the COSO framework: (1) criteria for assessment and (2) whether the report covered a point in time or a period of time. In addition, two of 80 companies specified the time period but did not mention the criteria. Ragahundan and Rama argue that the reason for insuffient information on the *effectiveness* of internal control may be management's perception of increased legal liability.

MacMullen et al. (1996) researched companies, which issued voluntary MRICs and tested the relationship between voluntary internal control reporting and financial reporting problems. They examined the proportions of companies with two types of financial reporting problems – SEC enforcement actions or restated earnings – *versus* all companies in the NAARS[11] database. They found that larger companies were more likely to report on internal control than smaller companies (assets less than $250 million) and small-sized companies with financial reporting problems were less likely to voluntary report on internal control. According to the authors, the results indicate that the benefit from mandating the reports on internal control may also be more useful for the smaller companies than for the larger companies, and they add that these results are consistent with the suggestion of the Treadway Commission (1987) that internal control problems may be greater in smaller companies and that the benefits from taking steps to improve internal control may also be relatively greater for such companies.

Hermanson (2000) analysed the demand for internal control by identifying nine financial statement user groups[12] and surveyed them to determine whether MRICs are useful, whether MRICs influence decisions, and whether financial reporting is improved by adding MRICs. The paper also examined whether responses varied based on the definition of internal control used (broad, operational definition vs. narrow, financial-reporting definition) and user group. Overall, the results indicated that financial statement users agreed that internal controls are important. Respondents agreed that *voluntary MRICs* improved controls and the oversight of controls, and provided additional information for decision making. Respondents also agreed

[11] the National Automated Accounting Research System (in the US)

[12] The nine groups (150 people) included: bankers, brokers, directors, executives, analysts, institutional investors, individual investors, CPAs, and internal auditors

that *mandatory MRICs* improved controls and oversight of controls, but did not agree about their value for decision making. Using a broad definition of controls, respondents strongly agreed that MRICs improved controls and provided a better indicator of a company's long-term viability. Executive respondents were less likely to agree about the usefulness of MRICs than the overall sample and executive mean responses were neutral as to whether mandatory MRICs motivate them to improve the control system. The CPAs, internal auditors, and executives were generally more familiar with the issues than the other user groups.

The Sarbanes-Oxley Act S404 has also “answered” to the question presented by Hermanson. Management’s reporting on internal control is mandatory and auditors have to attest to, and report on the assessment made by the management. Finally, although S404 regulates management assessment on internal control over financial reporting, the act has adopted the broad definition of internal controls by referring to the COSO framework.

5 METHODOLOGY AND DATA

This chapter introduces the research methodology of the study and describes data and the research methods applied throughout the empirical analysis. The chapter consists of three parts. The first part deals with the selected research method and the second part focuses on describing data by explaining what kind of material is used in the research. The third part provides a description of the research process.

5.1 RESEARCH METHOD

The research method of this thesis is a case study. Eisenhardt (1989, p. 534) defines that a case study is *"a research strategy which focuses on understanding the dynamics present within single setting."* Case studies can involve either single or multiple cases, and numerous levels of analysis (Scapens 1990, p. 264). In this study, only one case company is examined. A case study as a strategy is appropriate when the form of the research question is 'how' or 'why' (Yin 1987, p. 17). The empirical part of this study examines the following questions:

How is internal control organised and maintained in the company?
How does the Sarbanes-Oxley Act S404 affect internal control in the company?

Based on the problem structure, three main classes of research designs can be distinguished: exploratory, descriptive, and causal (Ghauri and Gronhaug 2002, p. 48). This study is a descriptive research, in which the problem is structured and well understood. The study relates to a practical problem of a phenomenon and its purpose it to describe it in a real-life context. A case study is, in fact, an empirical inquiry that investigates a contemporary phenomenon within real-life contexts (Yin 1987, p. 25). As already explained above, the purpose of the study is to depict the current practice in the case company and to describe the application of new procedures i.e. examine potential problems and of new rules and practices.

Because of the fact that the empirical study is carried out in one case company, the study includes small-scale data but in relation to the case company, an in-depth analysis on the data will be performed. However, this sets limitations and problems to the study. First of all, the greatest concern is the lack of generalisation and academic rigour (Yin 1987, p. 21). Because of the research method of this study, no statistical generalisation from a sample to a population can be made. Thus, results e.g. explaining how the S-O Act S404 has affected internal control in practice in the case company cannot be generalised to other companies. So in this study, any generalisation with relation to other companies cannot be made and conclusions are stated only in the case company context. The study will give some implications on what kind of difficulties, challenges, and benefits companies face when they are implementing these new requirements of internal control. In addition, due to the research method and a small sample size (12 respondents) of questionnaire, only descriptive statistics are introduced.

The researcher's relationship with the subject researched can be seen as a weakness of the empirical study. The researcher of this study has been working in the case company for a year and participates both in the case company's S-O project and internal control processes. It is inevitable that this affects both the objectivity of the study and the validity of evidence because the researcher has formed a view before the empirical study was conducted. The negative effect on validity is minimized by being aware of this weakness and it is emphasized both in the questionnaire and in the interviews that "the researcher acts independently and not as an employee of the case company". In addition, triangulation of data i.e. collecting data through different methods and using different kind of data, improves the accuracy of judgements and thereby results.

Certain ethical issues in the case study are important and these will also influence the research. These issues cover preserving participant's anonymity and preserving the case company from competitors. Access to information is well available but this also means confidentiality, which may cause problems in writing the thesis. All information cannot be written in this report because of its sensitivity in respect to competitors.

5.2 RESEARCH DESIGN OF EMPIRICAL STUDY

The empirical study is organised as follows. First, a suitable case company was selected. The only requirement was, in fact, that the case company has to be obligated to start complying with the Sarbanes-Oxley Act of 2002. This means that the company has to be a subsidiary of a public company in the US or the case company's shares have to be listed in a securities exchange registered with the SEC.

The second stage was collecting evidence, which includes a variety of documentation, direct observation, questionnaires, and interviews. The purpose of the empirical study is to examine the internal control system in the case company with the help of the COSO framework, which has been discussed in the literature review of this study. For this reason, the results of the empirical analysis are divided in five chapters as follows: (1) Control environment, (2) Risk assessment, (3) Control activities, (4) Information and communication, and (5) Monitoring. In addition, evidence is collected to make conclusions on how the S-O Act S404 has affected the case company's internal control processes.

The third stage is writing a report that is to describe the case company, present findings and make conclusions. Findings and conclusions are to illustrate the internal control system and the effects of S-O Act S404 on internal control of the case company. No generalisation can be made to other companies but some suggestions are presented on how the Sarbanes-Oxley S404 may affect internal control processes in general. Finally, the case report gives recommendations for the case company and on future research.

5.3 RESEARCH DATA

Eisenhardt states that case studies typically combine data collection methods such as archives, interviews, questionnaires and observations (1989, p. 534). The evidence may be qualitative, or quantitative, or both. The research material of this study includes (1) a questionnaire and interviews, (2) personal observation and notes, (3) archived records and documentations. Table 1 lists the research data collection method and the research material.

Table 1: The research material

Research data collection method	Research material
(1) Questionnaire and interviews (qualitative data)	* Questionnaire * Material of interviews
(2) Observations and notes (qualitative data)	* Direct observation * Personal notes
(3) Archived records and documentation (qualitative data)	* Minutes of meetings * Announcements and memorandums * Documents of the ICMP process and internal audits * Documentation of S-O project

The primary source of data is the questionnaire. Appendix 4 presents a covering letter and the questionnaire. The questionnaire is based on the five components of the COSO Framework and it consists of six parts: 1. Background information, 2. Control environment, 3. Risk assessment, 4. Control activities, 5. Information and communication, and 6. Sarbanes-Oxley. The questionnaire includes both open and multiple-choice questions. The multiple choice questions provide either 'Yes' or 'No' choices or a respondent is asked to rank answers in the scale of 1 to 5, where 1 is 'strongly agree' and 5 is 'strongly disagree'. The scale also includes an alternative 'can not say' (CNS). In order to examine the possible changes in the factors during the last two years, respondents were also asked to evaluate whether the factor has changed for the better '+' or for the worse '-'.

The questionnaire was sent to the leadership team of the case company and to the relevant employees at the finance department. There were twelve respondents, which are GM Nordic (acting also as GM Finland), three business operations managers, two sales managers, HR manager, country controller, logistic manager, invoicing manager, chief accountant and financial analyst. The questionnaire was written in Finnish for eleven respondents to ensure that they understand the questions clearly. One respondent does not speak Finnish so the questionnaire was translated into English. Considering that the author of this study is not native English speaking, the risk may be that the questions in English do not have exactly the same connotation as the questions in Finnish. It should also be noticed that the respondents expressed their own opinion on how they feel about the factor in question. Further, the sample consists only of twelve answers so results will not portray the absolute truth within the organisation but still, give indications on the case company's internal control environment and processes.

Research data includes personal observation, archived records and documentation, and two formal interviews as a secondary source of data. Because of the fact that the researcher is working in the case company and has day-to-day discussions about internal control with the respondents, it was not necessary to have more than two formal interviews. The secondary source of data is to supplement data or to find answers to the question 'Why?' if the answers in the questionnaire were somehow exceptional. The research material is described in Table 1.

6 EMPIRICAL ANALYSIS

6.1 INTRODUCTION TO THE CASE COMPANY

The case company is located in Finland and is an information technology firm that focuses on technology, workflow, and services. The company provides products such as software and digital systems to a wide variety of customers. Services cover consulting, workflow, and outsourcing. The company offers customers solutions, which help businesses to develop online document archives, analyse efficient ways to share documents and knowledge in the office, and build Web-based processes for e.g. direct mail, invoices, and brochures. Of these especially outsourcing services is a growing business. Competition for market share is extremely fierce with decreasing margins that leads companies to invest in coverage and distribution channels, for example.

The case company is owned by an UK company, which, in turn, is a subsidiary of an American public listed company in New York Stock Exchange. The headquarter of European companies is placed in the UK. The case company is a part of a Nordic organisation. The company has a country manager in Finland, who is responsible for e.g. organising and maintaining the internal control system. The general manager operates at a Nordic level and has an ultimate responsibility for internal controls of the case company. Operations are managed through a Nordic management structure, which is responsible for Finland, Sweden, Denmark and Norway companies. There are four separate business operations in the case company and administration covers human resources, logistic, and finance. The finance department includes customer administration, payroll, and planning & accounting. Business managers, HR manager and country controller report directly to Nordic first line managers. The company has a matrix organisation.

Accounting of the case company is done according to the Finnish GAAP but financial reporting to the headquarter follows the U.S. GAAP. Financial reporting is prepared according to the local generally accepted accounting principles once a year when the statutory annual statements are prepared. Monthly financial reporting consists of a profit and loss statement, a balance sheet, and balance sheet specifications, and it is prepared according to the

U.S. GAAP. Other monthly and quarterly reporting includes headcount and other more detailed reports such as tax, activity, and profitability reports. Financial information is consolidated in the European headquarter and reported to the corporation in the United States. Considering internal control and the achievement of the objective to comply with applicable laws and regulations, it is particularly important that the headquarter ensures that the reporting units are provided with all necessary information on U.S. GAAP and that they have appropriate knowledge of the compliance with U.S. GAAP. The compliance with applicable laws and regulations is ensured through accounting policy guidelines and specific newsletters, which are communicated to relevant people in the finance departments and are available on the intranet.

There are specific characteristics of organisation that are relevant in terms of internal control and financial reporting. These are e.g. different geographical locations and a variety of information systems. The case company is responsible for control activities relating to its operations and administration despite the fact whether a control is performed abroad or in Finland. For example, the entire accounting of one business unit is done in the UK, which means that all documentation of accounting is abroad. This situation may cause difficulties in the audits performed by independent auditors and tax authorities. In addition, accounting of this business unit is performed in a different information system, to which Finnish finance people do not have access. This example leads to an interesting question: how does the company in Finland ensure that internal controls are working efficiently if it does not have an actual control on it? Although the company in the UK organises and maintains internal controls of the unit, it is clarified that the ultimate responsibility remains in the case company in Finland.

Let's take another example. The inter-company accounting department of the European reporting units is located in Ireland. Although the inter-company accountants record transactions and do the reconciliation of balance sheet accounts, the case company is responsible for internal controls relating to its inter-company transactions. Also inter-company documentation is archived abroad. The IT system support gives a third example, which describes challenges faced because of different geographical locations. The support is located in the UK and given only in English. This may have adverse effect on internal controls. People performing control activities, e.g. running control reports in the information system, may face difficulties and they may not ask help easily, if they have to do that in English. Further, they may not understand the instructions clearly given by the system support. These aspects of communication should be taken into account because IT controls have a more and more important role in the internal control processes nowadays. On the other hand, the integrated information system SAP used in the companies gives visibility that enables more efficient internal control activities.

First, it is important to notice that people working in different countries have different culture and language that may affect mutual understanding, confidence and trust, and working methods. Secondly, the business model of the corporation is quite complicated covering services, equipment sales, and direct sales versus sales through distributors and resellers. Third, reporting relationships and authorisations can be quite complex in a Nordic organisation, in which the case company's managers report directly to their superiors at a Nordic level. These characteristics challenge the effectiveness and efficiency of internal control system.

6.2 IMPLEMENTATION OF THE SARBANES-OXLEY ACT S404

6.2.1 Project S404 at the European Level

The Sarbanes-Oxley project started at the European level in fall 2002. Reporting units were classified as three groups according to the scope of documentation and evaluation requirements: *comprehensive* ("Green locations"), *limited* ("Yellow locations") and *minimal* ("Red locations"). The criterion for the green locations was that a country is a material component of the overall corporate financial results. Yellow locations were required to review only specified significant accounts, where as red locations were defined as a reporting unit which is not significant to the overall assessment of internal control. The scope of green locations cover all cycles, while the yellow countries were required to cover only the revenue and accounting cycles. No S-O S404 documentation was required from red countries.

There were several areas - called cycles - that were considered significant considering the evaluation of effectiveness of the corporation's internal control system. The cycles consist of several processes and sub-processes and are as follows:

- Form 10-K/Q[13]
- Financial reporting cycle
- Accounting cycle
- Treasury cycle
- Purchases and payables cycle
- Revenue and receivables cycle
- Payroll cycle
- Production cycle
- Property, plant and equipment cycle

As discussed earlier in this study, the SEC Final Rule states that a company's management is required to base its evaluation of the effectiveness of company's internal control over financial reporting on a suitable and recognised internal control framework. The parent company in the U.S. has adopted the COSO Framework as its evaluation criteria. This framework was specifically pointed out in the SEC Final Rule and was also approved by the PCAOB as a suitable framework for management's assessment. However, it is emphasised in the company's internal control documentation that *"the company's historical and pre-existing internal control programs address all of the objectives of the COSO Framework"*, which are effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulation (Adoption of the COSO Framework, p. 1). The document adds that these internal control programs include entity level controls, e.g. the audit committee of the board, a strong tone-at-the top, the senior management audit committee, world-wide internal audit, disclosure committees, self inspection programs, ethics programs, HR practices, and financial planning & accounting activities.

---

13 The US federal securities laws require publicly traded companies to disclose information on an ongoing basis. The annual report on Form 10-K provides a comprehensive overview of the company's business and financial condition and includes audited financial statements. The Form 10-Q includes unaudited financial statements and provides a continuing view of the company's financial position during the year. The report must be filed for each of the first three fiscal quarters of the company's fiscal year. http://www.sec.gov/answers/form10k.htm and http://www.sec.gov/answers/form10q.htm

The project plan of implementing S-O S404 was divided into four phases. Figure 4 presents different steps in the implementation process and time scheduling of project. These steps follow Quall's five-step methodology. As the figure summarises, all significant processes and sub-processes of the cycles were documented. Also risks relating to these processes were identified and documented and relevant control activities determined to minimise these risks. As the S-O Act requires, testing of key controls and test plans were defined and the actual testing performed by the end of Q2-2004. Phase 3 included gap closure, if some weaknesses were detected. Next chapter introduces these phases in detail.

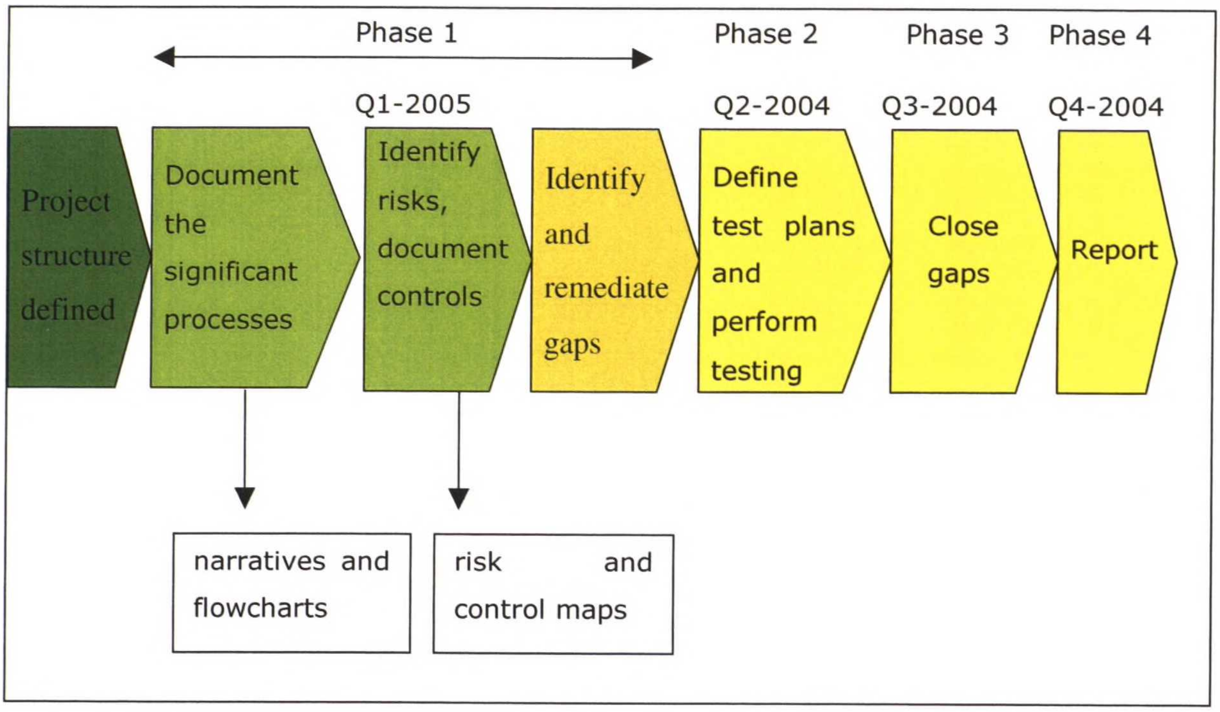


Figure 4: The implementation of the Sarbanes-Oxley Act S404

6.2.2 Implementation of S404 in the Case Company

In Finland the project was launched as a part of Nordic S-O project in May 2003. In practice, phase one was started in the beginning of 2004. The project team consisted of six members who all worked part-time in the project along with their existing work responsibilities at the finance department. An interesting point was that the Nordic countries were not separately significant but together the situation changed. As a result, the case company was considered as a location with a limited scope and it was required to document and assess two cycles: accounting cycle and revenue & receivables cycle. These cycles consist of several processes and sub-processes (see appendix 2 and 3).

First, processes were identified, documented and evaluated. Documentation was prepared by using narratives and flowcharts. Secondly, risks relating to the defined processes and sub-processes were identified and documented by asking the question "What can go wrong?". The project team considered that this phase was very difficult and that they did not get necessary support from the headquarter. They emphasised that after the project team had identified risks, they did not get any feedback whether these risks and controls were relevant and properly defined. Identifying risks is an essential and significant part of the project because if risks are not determined properly - they are incorrect or irrelevant - it will ruin the rest of the assessment process. If risks are not correct, control activities based on these risks will also be incorrect. This would be harmful considering that the purpose is to define proper and necessary control activities and put those in place to ensure that the objectives of the COSO Framework are achieved. If control activities are incorrectly defined, it is useless to test these controls. It is surprising to notice that there was no inspection at this stage of the project. This may follow from the fact that the case company was classified only as 'a yellow country' and that limited resources directed the headquarter to concentrate only on the significant countries.

After risk assessment, appropriate control activities were identified and documented. The case company's control activities were typed as preventative, detective, manual or IT. A control can be either a key control or a supportive control, and it can be performed daily, weekly, monthly, quarterly, annually, or constantly. Table 2 presents the identified risks and controls relating to the process of credit assessment. The process "Credit Assessment" is included in the revenue and receivables cycle (REV.004). The objective of credit assessment is to maximise receivables performance by minimising credit risk exposure and ensuring prompt payment terms. As the table shows, there are two identified risks in this process. The control description clarifies how the risk should be controlled, where as the last column describes the type of the control. Both of these controls are key controls and they are preventative. Constant means that the control is performed continually.

Table 2: The process of credit assessment, Risk & Controls

RISK	CONTROL DESCRIPTION	CONTROL EVIDENCE	TYPE OF CONTROL
1. Orders are created for customers, who are not creditworthy.	New customers are credit checked before the Sales Offer. Local Credit policy is communicated to the Sales Personnel.	Credit Check form approved and signed by Controller or Credit Controller according to the Authority Matrix.	Preventative Manual Key Constant
2. Customers, who are not able to pay, get service and consumables.	Customers with outstanding aged dept are blocked for any service/consumables provide in XSAP. Blocking is based on bankruptcy/debt restructuring/other corresponding information received from the authority Suomen Asiakastieto Oy.	System based control. Order is not completed in the SAP because of the block. All the blocked orders can be seen in the workflow in SAP and email received from the system when a new order gets into the SAP. All the information regarding companies with financial difficulties are filed by Credit Controller.	Preventative IT/Manual Key Constant

The next phase after evaluation of risks and controls is to define test plans and perform testing. Because of the fact that the case company was categorised as a yellow country, it was not required to perform testing. However, a decision was made at a Nordic level that all Nordic reporting units should prepare the test plans and perform testing. In Finland the test plans were prepared at the end of 2004 and they included the following information: (1) the description of cycle and process, (2) test period covered, (3) a detailed test procedure description e.g. sample size, criteria for a sample selection, (4) the description of tested control, and (5) control objectives.

Let's use the process of credit assessment as an example. The first risk was that orders are created for customers, who are not creditworthy, and the second risk was that customers, who are not able to pay, get service and consumables. The test procedure description of the first risk is: *"check 10 customers from and 3 months from the past to ensure that the Credit Control form has been approved by the Credit Controller and Controlled before the offer"*. The description of the second risk is: *"check that the credit block is active for a customer that has the adjudication in bankruptcy or has payment problems to the company"*. In general, a test plan answers questions 'why', 'how' and 'what'.

After specifying the test plans, actual testing is performed. It is vital that a test plan is defined properly in order to ensure that testing is done in a correct way and that a tester can not have an effect on the test results. Currently, the case company's status of S-O project is that the testing of every process and sub-process has been completed. According to the SEC rules, a company must report on internal control for every reporting period. Because of this, testing of key controls has to be an ongoing process. Actual testing will be a challenge for the case company because it requires time and people with appropriate skills. Finance staff should perform testing and it should be a part of quarterly performed tasks.

Although it is discussed in professional literature that operational managers should be a part of Sarbanes-Oxley projects and internal control processes, it is a fact that the case company's finance department alone has participated actively in the S-O project. There are only few exceptions in the leadership team. According to the interviews, people in the finance department are of an opinion that they are alone trying to meet the requirements of S-O Act without having much support from operations. They also feel that people are not interested in the S-O project or the internal control processes, in general.

The team members of S-O project consider that describing the company's processes, evaluating and assessing risks has given them a better understanding of the company's business and processes. It has also affected positively internal controls because finance are now performing control activities more consciously and knowing the purpose of certain control. As Farrell (2004) notes, internal control assessment may lead to greater use of controls, better evaluation of process risks and more uniform controls throughout the organisation.

6.3 RESULTS

The twelve respondents of questionnaire covered the leadership team and four people from the finance department. Seven of them participate in the Sarbanes-Oxley project in Finland and one respondent contributed to the S-O project in the UK. Nine respondents participate in the case company's internal control management process and of these respondents, five persons work in the finance department. Interestingly, only a part of the leadership team considered to be a part of the ICMP process, although the COSO emphasises that especially top management is responsible for internal control.

6.3.1 Control Environment

The COSO framework emphasises that control environment is one of the key components of internal control. It sets a tone within an organisation, influences the control consciousness of people, and is a foundation for all other components of internal control system. The tone at the top is a major factor in creating positive control environment. Management affects directly the control environment through its operating style, philosophy and ethical values. The first part of the questionnaire handles issues relating to the case company's control environment. These issues cover e.g. integrity, ethical values, incentives, reporting relations and authorities, a management's philosophy, and an organisation structure.

Integrity and Ethical Values

Ten of the twelve respondents agree that the case company's employees behave very ethically, while one respondent disagrees. About half of the respondents (7) consider that the situation has changed for the better during the last two years. All respondents are of an opinion that the employees are honest and reliable, except one respondent 'can not say', and 8 respondents consider that this factor has improved. Ten respondents consider that the company's ethical values are clearly communicated and nobody thinks that communication would have weakened during the last two years. One respondent replies 'can not say' to every question due to the fact that the respondent has just started working in the case company and does not have experience to rank these factors.

As COSO notes, it is essential that management effectively communicates the company's values and behavioural standards to employees. The corporation's business ethics are communicated to all employees once a year. This booklet clarifies ethical behaviour and the roles and responsibilities of employees and superiors. Business Ethics 2005 guidelines pay a lot of attention to revenue recognition. It also includes a separate section of control activities relating to financial reporting and to the compliance with laws and regulations. It states (p.6) that "*employees are expected to know the legal, policy and financial controls that apply to their jobs. You are responsible for: (1) keeping accurate financial records for all your transactions, forecasts and business assessments,(2) understanding the financial records and processes associated with your job, and (3) safeguarding company assets that are entrusted to you...*" These requirements relate directly to internal controls over financial reporting to ensure a true and fair view in financial reporting, and to safeguard company assets. Also the requirement of S-O Act to maintain supporting documentation and evidence comes up clearly.

The respondents were asked, whether they consider that the code of conduct is followed in *actual* behaviour. Answers to this question vary. Half of the respondents neither agree nor disagrees and one respondent strongly disagrees, while 4 respondents agree and one can not say. The COSO framework notes that a company's code of conduct can be just written instructions for what management would like to occur in the organisation. However, organisational culture defines whether the rules are actually obeyed, compromised, or not followed at all. Only fifty percent of the respondents agree and 3 persons disagree that non-compliance with the code is not accepted in the company. None of the respondents consider that this situation would have changed for the worse. The COSO framework states that management should create mechanisms that encourage employees to report suspected violations. The company has an ethics telephone line through which employees are able to inform violations anonymously. Based on the respondents' answers, it seems that although the ethical values are communicated efficiently, they are not imprinted on the employees and that there are no appropriate penalties. However, many of the respondents point out that they know how the code is followed in their function but they do not know how it is followed within the whole organisation.

The last question was, whether the case company's top management sets a good example for other employees by behaving ethically. Interestingly, only a half of the respondents agree, while a third of respondents disagree. Five of them consider that the situation has changed for the better, while 4 respondents are of an opinion that the change has been unfavourable during the last 1-2 years. This result is very significant considering the fact that if the top management is not committed to the company's ethical values, it is very likely that other employees do not consider these values important.

According to COSO, individuals may take dishonest and unethical actions if their organisation gives a strong incentives or temptations to do so. Interestingly, the framework further notes that emphasis on making revenue and profit especially in the short-term promotes environment in which individuals are trying to achieve the targets in every possible way. Eleven of the twelve respondents agree or strongly agree that making profit in the short run is emphasised in the company. Also ten respondents strongly agree that revenue growth is prioritised as the company's objective. This situation should be taken into account when establishing effective internal controls. The respondents were also asked if top and operational management are constantly aware of activities performed by their staff and if internal control processes properly ensure that misbehaviour is detected and reported. Answers to these questions vary a lot and no clear conclusions can be drawn. In addition, an average of four person do not rank their answers, whether the situation has changed for the worse or for the better. Because of this, no conclusions are made on the direction of change during the last 1-2 years.

Commitment to Competence

The respondents were asked, whether the company's top management encourages individuals to a good performance. Eight of them agree, while one respondent disagrees and three respondents neither agree nor disagree. It is interesting to notice that one third of the respondents do not consider that management encourages to a good performance considering the fact that the majority of respondents are this management. The questionnaire asked about the company's commitment to the competence of staff. Five respondents agree and five disagree that competence requirements are defined to different job assignments. Half of the respondents agree that individuals have sufficient skills to perform their work and 8 respondent consider that a competence is highlighted in recruiting. It is worth noticing that four respondents consider that individuals do not have sufficient skills to perform their work.

Board of Directors and Audit Committee

The COSO framework notes that a strong, competent and active board of directors and audit committee have a critical effect on the control environment. The role of the board of directors is not significant in a control context of the case company and the board is mainly to fulfil its legal responsibilities set by company law in Finland. The board consists of the UK company's CEO, the case company's CEO, finance controller, one sales manager, and one legal councillor. Additionally, there is no separate audit committee in the case company; the audit committee of European companies is in the UK. There is the operation managers' audit committee (OPMAC) in the company, which holds meetings quarterly. These meetings are a part of the company's internal control system. The OPMAC meeting is considered as a forum, in which all participants can and should present issues and problems relating to internal control. The meetings are led by the controller and the leadership team, operational managers and finance staff are required to be present. However, according to the participant lists in the minutes of OPMAC meetings it seems that it is the finance staff that attends to these meetings and the majority of the leadership team and operational managers are absent. This situation is also emphasised in the internal audit report 2004: "*It is important to realise that internal controls is a matter for all functions, not just for Finance. In this regard it is important that the* <u>*entire*</u> *senior management team attends the OPMACs and fully participates in the local ICMP process.*" (ICMP Validation Summary 2004).

One third of the respondents agree that the OPMAC is setting the tone in the organisation and influences significantly the control environment. Of these respondents, only one person works in the finance department. Fifty percent consider that the OPMAC is active and has an important role in assuring effective internal control, while 4 respondents disagree. A half of the respondents also consider that the situation has improved during the last 1-2 years.

It seems that the OPMAC is active because it is organised regularly and it handles issues effectively according to the "to do" lists and actions closed in the minutes of meetings. The problem seems to be with the commitment of other than finance people. According to the respondents working in the finance department, the OPMAC cannot have an important role and it will be quite useless as long as the top management does not attend the meetings. This is because of the fact that finance alone cannot solve internal control problems, which are often closely related to operations. The weak commitment of leadership team and operational managers indicates that internal controls are considered as the responsibility of finance. This way of thinking is not exceptional. As Farrell (2004) notes, there is conventional wisdom that the responsibility of internal controls is delegated to the finance staff of organisation.

Management's Philosophy and Operating Style

Surprisingly, only eight respondents agree that top management is honest and reliable, while 2 respondents neither agree nor disagree, and also 2 respondents disagree. Four of them consider that the situation has improved. Half of the respondents do not consider that the company's top management has taken a positive stand and that it is interested in effective internal control. Fifty percent consider that the situation has changed for the better, while four respondents are of an opinion that the change has been unfavourable. Seven respondents disagree that the top management sets an example for the staff or shows that effective internal control is important. Although the answers vary a lot in these questions, again the results indicate that there seems to be problems in the management's attitude towards internal control.

Half of respondents consider that the company is directed formally, while 5 respondents consider it to be informal. This may be due to people defining an informal versus a formal management style in a different way. The questionnaire did not define these alternatives clearly enough. However, 11 respondents consider that the management style has changed towards more formal than earlier during the last 1-2 years. It is very likely that the change is the effect of S-O that has e.g. caused a greater awareness of internal control and forced companies to tighten their internal control policies.

Organisational Structure

From an internal control perspective, it is relevant that authority and responsibility are assigned appropriately and that reporting relations are appropriate in respect to a company's objectives and the needs of the organisation. Eight respondents consider that reporting relations within the case company are clear, while 2 respondents disagree. The respondents were also asked, whether the reporting relations from the company upwards are clear. Half of the respondents agree and four of them disagree. Six respondents consider that the situation has changed for the worse during the last 1-2 years, while 2 respondents think that the situation has improved. Four respondents did no answer the question.

It is interesting to notice that half of the respondents do not consider the organisation structure as practical and that it does not support the achievement of the company objectives. One respondent points out that *"organisation is still changing and the organisation structure has not supported activities"*. Many of the respondents state that a Nordic organisation and a matrix organisation is unclear and complicated and that there are situations, in which it is not clear, how the process should work. One respondent gives an example by noting that *"there are several separate business operations in the case company that operate individually. Boundaries are unclear and there is a lack of cooperation"*. Another respondent considers that *"matrix organisation supports only the achievement of objectives of separate business operations"*. In addition, one respondent states that *"there are situations, in which the same matter is handled at a different organisation level causing a double work"*.

A Nordic organisation creates difficult situations, in which authority and responsibility do not go hand in hand. For example, a manager at a Nordic level is authorised to make decisions relating to the expenditure of the case company. However, it is the operations managers in the case company, who are responsible for the overstatements of budgets and cost savings. As a result, managers in the company may be responsible for actions, which they have not decided and approved. Another example is inter-company accounting and IT system support. Although these activities are centralised, it is the responsibility of reporting units in the countries to ensure that these activities operate properly.

Based on the results, the organisation structure is not considered as appropriate with respect to the case company's objectives and the needs of the organisation. The reason for this is that the case company is a small business unit in a global corporation and its operations are just a very small part of a big business. It is not a question of needs and requirements of the case company but of the corporation. A comment from one respondent summarises the reason for the organisation structure: *"I am aware that a Nordic organisation is not optimal for all* *processes but is best for creating a profitable unit."* It may seem inflexible to require small business units to apply the corporation's internal control guidelines, regulation, and the S-O requirements because small reporting units probably do not have enough resources to cope with these requirements. However, the compliance is important considering the overall picture: small reporting units combined together may be an important part of the overall corporate financial results. This is the case with the Nordic region and other minor European countries. On the other hand, being a part of a global corporation provides benefits. There are clear and extensive guidelines, on which a decision can be based and the headquarter gives support on difficult issues. Above all, internal control requirements should be seen as a benefit. If the company fulfils the requirements, it ensures effective and efficient operations, reliable financial reporting and compliance with applicable laws and regulations.

Assignment of Authority and Responsibility

Authorities and responsibilities are usually cascaded to different levels at the organisation. The COSO framework states that as a part of a control environment, it is a good practice to create operating principles or policies, and to write down the reporting relations and different authorities. Seven of the respondents consider that authority and responsibility is significantly cascaded to different levels within the company, while 3 respondents disagree. It is interesting to notice that only 5 respondents consider that reporting relations and authorisations have been written down and communicated clearly in the company. Eight respondents disagree that the employees are aware of the boundaries of authorities. In addition, half of the respondents consider that the change during the last two years has been unfavourable. For example, the ICMP validation summary 2004 notes as follows: *"some contracts are committed with the customer before review of Finance... there are a lack of adherence to price guidelines and a rather generous delegation of authority..."*

The respondents were asked, whether they consider that employees are encouraged to solve problems independently and the scope of authority assigned to the employees is appropriate. Seven respondents agree with both of these arguments. An individual's independency and the extensive scope of authority can be seen in two different ways. Independency may encourage employees to work more efficiently and commit them more to meet a company's objectives. On the other hand, some employees do not consider that an extensive scope of authority is a good thing because it brings a greater responsibility for the decisions made. The COSO framework reminds that the scope of authorities given to a lower level requires a risk assessment to ensure that the risk taken in authorisations is acceptable.

Human Resource Policies and Practices

The majority of respondents (10) agree that employees are encouraged to educate and develop themselves. The corporation has created an extensive e-learning centre in the intranet and e-learning includes courses covering separate areas such as business and operations, product knowledge, financial and accounting issues, business ethics, IT. The corporation also arranges many internal courses in a variety of learning areas and it acknowledges that development of the employees is very significant. As COSO notes, training policies illustrate the levels of performance and behaviour that a company expects from its employees. Commitment to education and development is important considering employees' know-how to improve operational, financial and legal processes and their engagement to the company objectives. These considerations are relevant also from an internal control perspective.

Internal Control Processes

The respondents were asked, who they consider to be responsible for internal control. The majority of respondents consider that it is the top management and finance. Only 3 respondent state that *all employees* in the organisation are responsible for internal control and 1 respondent does not answer the question at all. Next, the respondents were asked to describe their role in internal control and whether the role has changed. The respondents mostly state that they are responsible for controls of their function and that their job is to ensure that functions operate according to corporation's guidelines and requirements. Especially finance staff considers that they play a more important role in the internal control than earlier and that their responsibility for control activities has increased during the last 1-2 years. The majority of respondents consider that internal control has tightened and 1 respondent even writes that this is due to the U.S. legislation.

All respondents consider that internal control is very important. One respondent concisely notes that it is to ensure that the company operates effectively, while another writes that *"internal control provides or should provide a framework, in which a company* *operates...and it clarifies procedures and authorities".* One respondent simply states that internal control is important because it is emphasised by the corporation, while another notes that *"it is not possible to grow the organisation in a sustainable way without working internal controls".* This statement also expresses clearly the company's priority to grow business. One respondent even considers that such a person should be employed to the case company, who would concentrate entirely on the internal controls, security and quality.

Different from other responses, one respondent states that *"internal control should be supportive not a decisive factor. When controls disturb our customers, it is too much."* For example, internal control guidelines require the following: *"Units should take steps to actively search for side-letters[14] by taking samples of customers to confirm terms and conditions of contracts. Such samples should include both a general random sample from all customers and narrower sample from those customer groups which experience suggests are particularly risky in this matter."* (internal documentation of the case company: 2005 Critical Control Checklist, Completion Instructions & Validation, 2. Contract and Order Control, p.3). The risk is that side letters' are issued to customers that may invalidate certain terms and conditions of their contract and as a result, revenue may be incorrectly recognised. Let's consider, how to put the requirement into practice. First, someone from the company contacts a randomly selected customer, with whom a contract has been made e.g. two years ago. They go through the terms and conditions of contract together and make sure that they both have the same conditions. Several problems and unpleasant situations are faced. First of all, this kind of manner is not a business practise in Finland. Customers may wonder why the contact person wants to go through the contract, which has already been agreed and signed the years ago. The customer may suspect that there is something wrong with the contract or he or she may even suspect that the contract has disappeared. In addition, the customer may become frustrated with spending time on an unnecessary checking. This requirement has been experienced particularly difficult to carry out without embarrassing the company. However, regardless of business practice or customer's point of view, this control has to be performed in order to fulfil the internal control requirement. As the example describes, there are cases, where internal control activities are not supportive but override business and customer

[14] A side-letter is defined as any unauthorised agreement with a customer (verbal or written) that resides outside and separate from the main agreement. 2005 Critical Control Checklist, Completion Instructions & Validation, 2. Contract and Order Control, 2.3 Side-Letters.

satisfaction. These controls may only be performed to meet internal control requirements and that should not be the purpose of control activities.

Summary

As it was discussed in the literature review of this study, there is a lot of confusion over the meaning of internal control and specific terms and concepts. Many respondents note that some terms in the questionnaire were not easy to understand and therefore they could not rank their answers. Some concepts of internal control, such as *control environment*, *internal control processes*, *risk management* or *a tone at the top,* are not unambiguous and they are not necessarily easy to understand in practice. However, the researcher of this study intentionally chose not to explain all terms and concepts in the questionnaire. The reason for this decision was that the researcher also wanted to examine the respondents' knowledge of internal control in general. There were quite a lot of answers 'can not say', 'neither agree nor disagree' or no answers at all. This may indicate that the respondents are not familiar with the concepts of internal control and that e.g. the leadership team has not a deep knowledge on internal control.

The COSO framework emphasises that it is significant to communicate the code of conduct within the whole organisation. According to the respondents, the company's ethical values are communicated effectively to the employees. The effect of S-O Act on the control environment can be pointed out in the corporation's communication on Business Ethics 2005, in which it is separately expressed that employees are responsible for safeguarding company assets and for legal, policy, and financial controls. However, it seems that the compliance with the code of conduct is not imprinted on the employees of the case company and there are issues with the tone at the top.

The COSO framework states that reporting relations should be clearly written down. Also authority and responsibility should be assigned properly at the different levels of organisation to ensure efficient and effective operations, financial reporting and the compliance with laws and regulation. The reporting relations upwards are considered as complicated in the case company and according to the respondents, the reporting relations and authorities are not clearly written down and communicated. In addition, there seems to be some problems with employees not having a clear understanding of their authority to make decisions. It is also considered that the organisation structure does not support the company's objectives and needs.

Although the majority of respondents consider that the top management and all employees are responsible for internal control, it seems that it is the case company's finance staff, which takes care of internal control processes in practice. However, most respondents consider that their role and responsibility in internal controls has increased during the last two years. According to the respondents, internal control has tightened in the company and obviously, this is mostly because of the S-O requirements.

6.3.2 Risk Assessment

The second component of the COSO framework is risk assessment. As the framework emphasises, the establishment of company's objectives is a precondition to risk assessment. These objectives can be clearly defined or they can be implicit. The questionnaire asked respondents to rank their answers, whether they consider that the case company's operational, legal and financial objectives are clearly defined and efficiently communicated. The questionnaire also asked about risk assessment in the company.

Objectives of the Company

The COSO framework states that it is very important that management pays carefully attention to identifying and analysing risks at different organisation levels and take actions to control them. The majority of respondents (9) agree that operational objectives and objectives relating to the compliance of laws and regulation are clearly defined and effectively communicated to the employees. Nine respondents also agree that the company's top management invests time in defining objectives and communicating these objectives within the company. The average of seven respondents considers that these factors have changed for the better during the last 1-2 years.

All respondents agree that the employees are committed to the company's operational and financial objectives. Seven respondents consider that the change has been favourable in the last two years (five of the twelve respondents do not answer the question). Nine respondents consider that the employees are committed to the legislative objectives of the company, while 1 respondent neither agree nor disagree and one of respondents disagrees. Five respondents consider that the situation has improved during the last 1-2 years.

As the COSO framework defines, internal control is designed to provide reasonable assurance regarding the achievement of objectives, e.g. operational objectives. The corporation has defined the performance priorities for 2005 as follows: *"improve customer experience, grow revenue, improve profitability and cash flow, create great employee experience, and live the values within the organisation"*. These are a common set of the objectives within the whole organisation so these are also the case company's objectives in 2005. By continuing to improve the customer experience, the company's aim is to retain and grow the customer base, which in turn, will generate revenue. According to the business directions, profitability and cash flow will be improved through disciplined cost and margin management, revenue growth and the pervasive use of Lean Six Sigma[15]. According to the Nordic mission, the aim is to double the revenue of one business area in two years and to achieve market leadership in two other business areas. In addition, the mission is to achieve 50 percent growth in profit from operations in 2005-2007. Considering these objectives, it is obvious that the ultimate goal for the year will be aggressive revenue and profitability growth.

There are also two non-financial priorities for 2005. *"Creating a great employee experience"* means that the aim is to create more a positive working climate within the organisation and to promote opportunities for people, leadership development and enhance two way communication of strategy and directions. *"Living our values"* includes the objectives to ensure the compliance with the Business Ethics policy, the code of conduct, the Sarbanes-Oxley Act, Lean Six Sigma, and to promote efficient work practices through process rationalisation and improvement. These objectives indicate that the company focuses also on

---

[15] Lean Six Sigma is a structured approach to identifying and eliminating defects in a manufacturing or office process. It is a quality management program to achieve "six sigma" levels of quality. It was pioneered by Motorola in the middle of 1980s and has spread to many other companies. Six Sigma aims to have the total number of failures in quality, or customer satisfaction, occur beyond the sixth sigma of likelihood in a normal distribution of customers. Here sigma stands for a step of one standard deviation; designing processes with tolerances of at least six standard deviations will, on reasonable assumptions, yield fewer than 3.4 defects in one million. The corporation of the case company launched this program in 2002.

committing the employees more and more to the organisation and to ensure the compliance with the company policies and laws and regulations.

From internal control perspective, a couple of considerations should be taken up regarding the objectives to grow revenue, commit employees more to the company, and comply with regulations. First of all, emphasising aggressive revenue growth, especially in the short run, may have an adverse effect on control environment. It may provide a negative incentive to the employees and an individual may try to achieve the objective every possible way by using disapproved methods. Appropriate incentives and effective controls should be defined and put in place to ensure that the risk of using disapproved methods would not occur. Secondly, focusing on improving the commitment of employees may have a positive impact on internal control. By indicating that the company values its employees and is willing to develop and support them, the staff will be more committed to the company. The staff may commit more to achieve the company's objectives and e.g. ethical behaviour. Finally, the company's business directions prioritise an issue, which is also emphasised in the COSO framework: the compliance with applicable laws and regulations. This is one objective of internal control and it also relates to reliable financial reporting. Considering internal control, it is relevant that the company stresses this objective.

It is essential to the achievement of efficient internal control that the company's objectives are communicated throughout the organisation. Management has to ensure that all employees are committed to the objectives. A program called *"Performance Excellence Plan"* is carried out in the corporation and every employee of the case company works with their managers to develop own Personal Excellence Plan (PEP) to support Nordic 2005 objectives. With the help of this plan, performance objectives are spread throughout the organisation to become performance objectives of every employee. The plan includes the company's goals, objectives, measures, and targets. It is important to ensure that there really is a deep understanding of these objectives. Managers organised specific meetings in the beginning of the year 2005 to review these objectives with their teams. As presented earlier in this chapter, the respondents consider that the company's objectives have been communicated clearly.

The respondents were asked to rank their answers, whether the company's objectives of compliance with the Sarbanes-Oxley Act are clearly defined and communicated. The majority of respondents (9) disagree with the argument. This result is not surprising because people, in general, are still not familiar with the S-O Act. In 2005, there have been cases that an employee has never heard about the S-O. In fact, even staff in the finance department, does not consider having a deep understanding of S-O Act. It seems that they are trying to implement the S-O requirements set by the headquarter but receiving only a little information, support and feedback.

Risk Assessment

The questionnaire asked about the risk analysis methods in the case company. The answers vary a lot. Eight respondents, of which five work in the finance department, disagree that management invests time in identifying and analyzing organisational risks and takes actions to manage those risks. However, 4 respondents agree with the argument. Five of the twelve respondents consider that identifying and analyzing risks is a more and more important part of their work. Half of the respondents disagree that the methods of risk assessment offered by the company are good. In general, the answers indicate that the respondents are not familiar with risk assessment or risk management.

As Farrell (2004) summarises, the evaluation and monitoring of business risks may help companies meet strategic goals and focus on corporate governance at the same time. By assessing risks and controls and documenting the descriptions of operational and financial processes companies may better understand their activities. He further notes that the responsibility for internal controls was formerly delegated to the finance staff but according to current thinking, internal controls should be owned by those, who manage daily operations and who depend on the controls for achieving their goals. The control process owners have the best knowledge to identify, evaluate and assess the possible risks.

6.3.3 Control Activities

The third component of the COSO framework is control activities. The framework presents that control activities are policies and procedures, which help ensure that management directives are carried out in the organisation and that necessary actions are taken to address risks to the achievement of company's objectives. The respondents were asked to describe control activities they consider significant in their work. Several controls are listed but the respondents clearly emphasise controls relating to revenue recognition. One respondent states that *"the most important control activities relate to revenue recognition and the procedures of the reconciliation of balance sheet accounts"*. Revenue recognition criteria are considered very important in the case company. The case company's internal control guidelines focuses on the revenue recognition aspects of the areas such as sales cut-off dates, correct calculation of accrued or deferred revenue, and sales and lease cancellations (2005 Critical Control Checklist, 6. Revenue Recognition, p. 1).

The COSO framework notes that control activities can include a variety of approvals, authorisations, verifications, reconciliations, physical controls, reviews of operating performance, security of assets and segregation of duties. Controls can by typed as preventative, detective, manual, IT or managerial control. One respondent is of an opinion that the following control activities are significant: approvals and signatures, balance sheet reconciliation, checklists such as FAS 13, and performance analyses. These controls include both preventative (approvals), detective (checklists, reconciliation) or managerial controls (performance reports). The company's internal control guidelines on margin management state that a unit should have *"an effective documented process to ensure that <u>all</u> contracts provide an acceptable rate of return to the company over their lifetime"* and it further emphasises that control needs to be exercised at two levels: at the outset of the contract and during the lifetime of contract (2005 Critical Control Checklist, 5. Margin Management, p. 1).

One respondent summarises that *"the foundation of all (internal control) is the segregation of duties and IT controls"*. Also another respondent emphasises the importance of IT controls and states that the most significant control activities are control reports provided by the SAP system. Ten respondents consider that the number of IT controls relating to operations and financial reporting has increased during the last 1-2 years. In addition, one respondent writes that the assumption is that data in the SAP is correct. These comments lead to an interesting question: how it is ensured that data in the system is accurate and correct? According to the internal control guidelines on information technology, there should be control over IT systems and applications such a way that the IT environment meets the S-O requirements. Access should be restricted to authorised personnel only and the access of those personnel should correspond to their roles and responsibilities. The IT controls include e.g. the segregation of duties[16] and a periodic user access review by business process owners. (internal documentation: 2005 Critical Control Checklist, 16. Information Technology, p. 1-2). In addition, only few people in the IT department in the headquarter have access to update master data in the system. According to the IT department, this restriction is due to the Sarbanes-Oxley requirements.

Some respondents consider that monitoring of contracts and pricing is an important control. A respondent writes that *"contracts are made carefully and no unclear conditions and terms are accepted! More attention is paid to payment terms..."* Also the pre-approval process of exceptional sales contracts is considered significant. Another respondent lists activities, such as *"pricing authority and monitoring of correctness of pricing and contracts"*. The case company's internal control guidelines on contract and order control focus on the following areas: new contract approvals, contract changes, side-letters, and creditworthiness of customer. (2005 Critical Control Checklist, 2. Contract and Order Control, p. 1-4).

One respondent highlights cost control. There has been a substantial focus on cost savings in the case company in 2005 and management and finance has invested time on improving cost management. Cost management includes e.g. appropriate signatures and authorisations in cases like pre-approval of marketing activities, training, customer entertaining, or permission to travel. Also authorities register is updated continually to ensure that there is updated information on, who is entitled to approve cost items. Detective cost control activities include e.g. monthly comparison of actual expenditure versus budget and prior year with the controller and cost centre managers. Any overstatements of budgets are investigated and corrective action taken if necessary.

The questionnaire asked the respondents, whether the company's top management pays attention to control activities. It is interesting to notice that only half of the respondents agree that the management pays a lot of attention to control activities, while 5 respondents have an

---

[16] The separation of duties so that people are not authorised to perform or have access to conflicting applications or transactions that may expose the company to financial risk or fraud.

opposite opinion (one respondent neither agree nor disagree). Fifty percent also consider that the situation has changed for the better during 1-2 years, while 3 respondents are of an opinion that the change has been unfavourable. It may have adverse effect on the company's control environment if the staff feels that top management is not interested in organising and maintaining controls. It is very likely that if top management does not highlight the significance of controls, the staff may get the impression that control activities are not important.

The respondents were asked, whether they consider that the segregation of duties (SOD) is sufficient so that errors and improper behaviour can be avoided. The answers vary a lot. One third of the respondents agree, while 5 respondents disagree and two respondents neither agree nor disagree. It seems that operations managers have an opinion that duties are appropriately separated. The respondents working in the finance department consider that the SOD is not sufficient. The reason for the results may be that the case company's finance organisation is flat when it is unavoidable that people are performing tasks with the SOD conflict. In these circumstances, appropriate control activities should be in place to ensure that risks relating to the SOD conflict do not realise.

All respondents consider that the number of control activities relating to both operations and financial reporting have increased during the last 1-2 years. However, none of the respondents listed any new control activities, which would have taken in place due to the S-O Act. It is clear that the S-O requirements have increased the number of controls. The act has also forced the case company to identify, document and test critical control activities. Although there would be no new controls separately created in the case company, the S-O Act has added knowledge and consciousness of existing controls – at least in the finance department.

6.3.4 Information and Communication

The fourth component of the COSO framework is information and communication. The questionnaire covered questions on the quality of information and communication efficiency. Eight respondents consider that information they receive is right and reliable, while three respondents have an opposite opinion. Seven respondents are of an opinion that information is open. By this it is meant that information is obtainable by appropriate parties and that the employees is getting all relevant information in order to perform their work well. An interesting result is that many respondents (7) consider that they are not getting information timely. Half of the twelve respondents also consider that they do not always receive the latest information. Yet, 7 respondents are of an opinion that the quality of information has improved during the last two years.

Nine respondents consider that superiors have a clear interest to listen employees and that they want to know about the problems (3 respondents neither agree nor disagree). It is worth noticing that none of the respondents disagree with this argument. The fact that superiors are interested in their staff, creates good working climate and employees feel that they are supported. This in turn, may commit employees more to the company's objectives. Seven respondents consider that employees have the means of communicating significant information upstream, while two respondents disagree. The answers vary a lot when the respondents were asked, whether the staff knows their responsibility in the internal control system or whether it knows how an individual work task relates to the work of others. As a result, no clear conclusions can be made on these questions.

Six respondents agree that top management has given a clear message to the staff that control responsibilities have to be taken seriously. Four respondents disagree with this argument, while two respondents neither agree nor disagree. It is also interesting to notice that 5 respondents consider that the change in this factor has been favourable during last 1-2 years, while 4 respondents are of an opinion that it has been unfavourable. Unfortunately, four respondents on average do not tell their opinion on, whether communication and the quality of information has improved or weakened during the last 1-2 years. Because of this, no clear conclusions can be made on the direction of change.

6.3.5 Monitoring

The fifth component of the COSO framework is monitoring. The framework states that a company's internal control system has to be monitored to assess the quality of the system's performance over time. Monitoring should be accomplished through ongoing monitoring activities and separate evaluations. The case company's ongoing monitoring activities include e.g. OPMAC meetings, financial reviews, reconciliations, comparisons, approval and authorisation register, performance reports, and other management and supervision activities. These controls have already been presented in the chapter "Control Activities" (6.3.3) of this study.

Considering the S-O S404, a relevant question is how the case company's monthly financial reports are monitored to ensure reliability? The financial reports naturally include a P&L statement and a balance sheet with its specifications. Month-end reporting activities include P&L and balance sheet review by the controller before releasing the reports to the headquarter. This review is the most important monitoring activity relating to monthly financial reporting and the correctness of reported figures is ensured through this review. Finance controller and financial analysts, who perform the actual reporting, review the P&L statement. Deviations from trends and expected results are investigated and corrections made if necessary. This monitoring activity can also be considered as a control, by which it is assured that the risk of unreliable financial reporting does not realise.

Balance sheet reporting is currently playing a more and more important role in companies' financial reporting. This is the case also in the case company and it can be seen in the internal control requirements set by the headquarter. For example, the controller should review beforehand all the balance sheet specifications schedule by schedule[17] according to the ICMP requirements. This requirement is hard to fulfil during the reporting in a tight month-end timetable with limited resources. At the moment, controller and chief accountant review the balance sheet account by account and this review is performed before preparing and releasing the balance sheet.

The company's monitoring activities include separate evaluations of the internal control system. The COSO framework notes that the scope and frequency of separate evaluations depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. The greater the scope and efficiency of ongoing monitoring activities is, the less

---

[17] The balance sheet specifications include altogether 25 monthly schedules. There are schedules for e.g. fixed assets, tax account movements, equity investments, intangible assets, and pension disclosures.

separate evaluations are needed. Separate evaluations can be directed to an individual control activity or to the entire internal control system. The most important separate evaluation is performed by an internal audit group based on a risk assessment and plan approved by the audit committee of the board of directors. Internal audit is performed once a year and it includes a comprehensive evaluation of both the internal control system and individual controls. Internal audit is called as ICMP review because it covers all the areas of internal control management processes in the company. As the corporation has based its internal control programs on the COSO framework, the work of internal audit focuses on the following control objectives: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

Formerly, the ICPM process has been separated from Sarbanes-Oxley documentation, assessment and testing. However, to minimise the duplication of work the ongoing requirements of S-O S404 are incorporated to the new process of ICMP review in 2005. This means that the case company has to assess also other cycles besides S-O cycles (revenue and accounting). It is relevant to notice that the internal control checklist[18] includes also certain operational and compliance controls, where as S-O S404 focuses on financial controls. The S-O cycles have already been discussed in presenting the S-O S404 project. Table 3 compares the S-O cycles to the critical control processes of ICMP in 2005. The ICMP Critical Controls Checklist 2005 - Guidance Notes remind (p. 1) that although the checklist mostly consists of processes that have already existed in prior years, many of the control requirements have been considerably 'refreshed' to fulfil the S-O requirements. As a result, the checklist includes the standard S-O key controls.

For many reporting units – including the Nordic countries - the scope of S-O has been limited to certain cycles only. The 2005 checklist will return to cover all cycles and standard S-O key controls. However, for those units outside the scope of S-O testing, a minimum level of S-O type testing will be required and this testing includes only certain key controls. In practice, the

---

[18] There is a uniform internal control checklist in all reporting units of the corporation, which define the processes and sub-processes of the internal control management process (ICMP). The checklist identifies the minimum control requirements to ensure that the necessary controls are in place and operating effectively. Internal audit and a company's assessment of effectiveness of its internal control are based on this checklist.

testing includes a certain amount of contracts, manual journals and balance sheet reconciliations.

Table 3: S-O cycles versus Critical Control Checklist 2005

	Entity Controls
REVENUE AND RECEIVABLES CYCLE	Contract and Order Control Billing Agency Billing Margin Management Revenue Recognition Accounts Receivable
ACCOUNTING & FINANCIAL REPORTING CYCLES (S-O S404)	Accounting and Financial Reporting
TAX CYCLE	Taxation
TREASURY CYCLE	Treasury Management
PURCHASING & PAYROLL CYCLES	Disbursement Authorisation
PRODUCTION CYCLE	Inventories
PROPERTY, PLANT AND EQUIPMENT CYCLE	Fixed Assets Control
IT CONTROLS	Information Technology
OTHER	Securitisation and Business Arrangements Business Security

In the ICMP review internal auditor evaluates strengths and areas for improvement in each of the processes and gives overall comments and recommendations. The case company's ICMP validation summary 2004 emphasises that the major weaknesses are top management's weak commitment to internal control process, the lack of adherence to price guidelines and "*a generous delegation of authority*". On the other hand, there are several strengths, which include e.g. a strong local process in treasury management and account reconciliations. Also credit note approval and review process is good and the summary states that the margin management has improved significantly compared to prior year. After ICMP reviews of all reporting units in Europe, individual unit ratings are determined. The ICMP ratings are roughly divided into four categories: A (good), B (moderate), C (weak), and F (no opinion can be determined). In the last four years, the case company's internal controls have been rated as A **"Good level of control, good protection against control failures"**. This means that the unit is able to demonstrate a high level of controls and sustainability over time. Weaknesses are limited in number and seriousness, with no critical weakness. So according to internal auditors' evaluation on the internal control system efficiency, the case company has good controls.

The COSO framework emphasises that internal control deficiencies should be reported upstream. Serious matters should be reported to top management and the board. After the ICMP review, a reviewed unit receives a ICMP validation summary, in which internal auditors state their opinion on the weaknesses and strengths in the internal control system of the audited unit. These statements are gone through in the OPMAC meetings and action plans are developed to address the weaknesses. In addition, internal auditors report all significant matters to senior management and the Audit Committee.

There are also other separate evaluations besides the ICMP review. These evaluations include at least an annual revision of statutory accounts, audits of tax authorities, and 'world wide audits' (WWA). The WWA's are performed by external auditors and a specific are of inspection is determined for every audit. For example, the scope of WWA in 2002 was significant financial processes with particular emphasis on revenue accounting, receivables management, and financial controls including account reconciliation processes. In 2005, there will be a WWA concentrating on the reconciliation of balance sheet accounts. These separate evaluations are not discussed further in this study.

Summary

The case company's monitoring includes a variety of separate evaluations of the internal control system, of which the most significant is the annual ICMP review. Internal auditors monitor the quality of the system's performance over time to assess the company's internal control management processes. They also monitor individual controls in detail. As the internal control programs are based on the COSO framework, the work of internal audit focuses on the following control objectives: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

Earlier the ICPM process has been separated from the Sarbanes-Oxley. However, in 2005 the critical control checklist has been redesigned to incorporate the ongoing requirements of S-O S404. This is because from 2004 onwards, the S-O Act S404 requires all reporting units to conduct an assessment of the effectiveness of their internal controls and to test the key controls. In addition, as the ICMP 2005 Critical Controls Checklist - Guidance Notes state, these conclusions are incorporated in the Corporate US GAAP financial statements, and are therefore subject to review by the independent auditors.

Sarbanes-Oxley requirements have changed the approach of assessment of internal control. It emphasises risk assessment and identification of control activities to defined risks. There should be key controls identified to significant risks. In prior years, the ICMP reviews have directly focused on assessing certain control activities and identification of risks has not been separately stressed. There has been, of course, underlying assumptions on risks to occur if controls are not in place but S-O requirements have brought a greater awareness that internal audit should be based on risk assessment. The effects of S-O on monitoring will be discussed in detail in the summary and conclusions of this study.

7 SUMMARY AND CONCLUSIONS

In recent years and throughout the history of several decades, there has been fraudulent financial reporting involving well-known corporations in Europe and in the United States. Currently, there is a growing public and professional interest on companies' reliability of financial reporting. Because internal controls are a precondition to reliable financial reporting, there is a growing interest in the internal controls of public companies nowadays. The concept of internal control has been, and still is quite unclear in practice.

The Sarbanes-Oxley Act of 2002 was enacted in the US. Particularly, Section 404 sets enormous requirements for companies, which are within the scope of the act. The act applies to the companies whose shares are listed in a securities exchange registered with the SEC. This means that the act has a global impact because it applies also to e.g. Finnish companies listed in NYSE or to the companies, which are subsidiaries of companies within the scope. The objective of the thesis was to depict the effect of the Sarbanes-Oxley Act of 2002, S404 on internal control practice. The value of this study is that it builds understanding on the concept of internal control, essential laws and regulations relating to internal control, and internal control practice. This study addresses the challenges and benefits of the Sarbanes-Oxley Act S404 that management faces in practice.

7.1 KEY FINDINGS OF THE THESIS

First, this chapter brings together the key findings of the literature review, prior empirical research and the empirical findings of this study. Second, it presents the managerial implications by dividing the recommendations into three classes. Finally, the chapter discusses the reliability and generalisation of the findings and makes suggestions for future research.

7.1.1 Key Findings of the Literature Review and Prior Empirical Research

The concept of internal control has been and is quite vague. As Maijoor (2000) claims this lack of clarity applies to both internal control practice and research. Thus, it is not surprising that directors and auditors were reluctant to make statements on companies' internal control when the concept of internal control effectiveness was very unclear in the past. The meaning and the scope have evolved over time but a trend from a narrow definition toward a broader scope definition can be observed. Internal control is considered to be a part of a company's corporate governance system, but the way the objectives of internal control are defined depends on whether it is discussed from an auditing perspective or from an organisation theory perspective. According to Maijoor (2000), the former concentrates on the effect of accounting controls on the reliability of financial reporting, where as the latter takes a broader view than auditing research. For example, the COSO and CoCo frameworks take a broader view. They extend the scope of internal control by discussing e.g. ethical values, attitudes and commitment of employees and other factors that relate to corporate culture. As Spira and Page (2003) state, the boundaries of the scope remain problematic. The empirical results of this study support the view that the concept and objectives of internal control are still quite vague.

In the light of recent developments, especially the Sarbanes-Oxley Act of 2002, an interesting question can be presented: *"Should there be laws or codes to ensure effective internal control of companies?"* The enforcement of the S-O act has caused the fact that some public companies are not able to make a choice anymore, whether or not they decide to comply with the codes. Recommendations and codes enable flexibility, whereas laws do not accept any justification for deviation from a recommended conduct. Further, the recommendations and the codes are to supplement laws and they just encourage companies to use best practices. However, this non-mandatory nature of codes gives companies an option, whether or not they will comply with the code. Additionally, the recommendations themselves give a choice to the companies not to comply with best practices if they believe that their situation justifies a different treatment. Nevertheless, management must give explanations why it has not complied with the code.

Legislation and regulations provide a basis. This means that they set a minimum standard of internal control that companies must comply. The level of compliance is decided by the management but several unconscious and conscious factors, such as attitudes, ethical values, management's operating style, the history of a company, determine this choice. Thus, the answer to the question, whether it should be self-regulation or forced legislation to ensure the effective internal controls, is mainly determined by the companies' control environment. For example, if there is a positive attitude toward internal control within an organisation and the management pays attention to risk assessment, control and monitoring activities and efficient communication of internal control, it is likely that the implementation of the S-O act requirements has not been difficult in the company. On the other hand, the act will have an essential effect on those companies, which have had inefficient internal control systems beforehand and forces these companies to significantly improve their internal control practice.

Finally, it should be noticed that different ownership structures, legal traditions, culture and business practices in different countries set a limit to the global convergence of internal control and corporate governance practices. These factors should be taken into account in legislation. The SEC Final rule of the S-O act recognises the problems faced by foreign companies with language, culture and organisation structures that are different from what is typical in the U.S. The rule gives additional relief for these companies by extending the compliance dates.

7.1.2 Key Empirical Findings

The employees of the case company are reliable and honest. The COSO framework emphasis two factors, which are essential in ensuring ethical behaviour within the organisation. These are top management's commitment to ethical values and effective communication of the company's values. The code of conduct, including ethical values and behavioural standards, is clearly communicated to the case company's employees. The company's code of conduct expects employees to perform certain control activities that are also required by the Sarbanes-Oxley act S404 – to maintain accurate financial records, understanding financial processes, and safeguarding company assets entrusted to the employees. Interestingly, the company's code of conduct is not followed effectively in the actual behaviour and it seems that there are not sufficient penalties for employees who violate the code. The employees may interpret that improper behaviour is acceptable and therefore, weaken the significance of the code within the organisation.

It seems that there are issues with the case company's management not fostering ethical behaviour by their example. This will eventually have an adverse effect on the case company's employees attitudes towards ethical values. Additionally, the situation has not improved during the last two years. According to COSO, management's integrity and commitment to ethical values is the most significant factor in creating positive control environment. People imitate their leaders and they are likely to develop the same attitude towards internal control as top management. It seems that the S-O act S404 has not increased the control consciousness of the case company's management. The empirical study of this thesis supports the conclusions made in prior researches that the operations managers do not usually consider themselves to be responsible for internal controls and that it would be the responsibility of the finance department. Additionally, it seems that all members of the top management do not consider that they are participating, or should participate in the implementation process of S404. The work of the case company's operation managers' audit committee is not effective although it addresses problems relating to the internal control system of the case company. Inefficiency of the OPMAC is caused by the fact that all managers of the leadership team do not attend the meetings. Again this result indicates that internal control is not considered as a matter of all functions.

Competence of individuals is highlighted in the recruiting process. According to COSO, this indicates the company's commitment to competent and trustworthy people. It is also worth noticing that the S-O requirements set higher competence levels to individuals who perform the work of identifying, assessing and testing the risks and controls of a company. It seems that management should specify more clearly the appropriate competence levels to particular jobs and translate them into required knowledge and skills. This is important, as the competence of the case company's employees will have a direct influence on internal control because it determines how well the job is done. The company encourages its employees to educate and develop themselves and has created several effective ways to support this personal development. As the COSO framework notes, this indicates that the company considers it important to signal its employees the expected levels of performance and behaviour. This in turn will create a more positive control environment.

The management style of the case company has changed towards more formal in the case company during the last two years. The fact that the S-O S404 has forced companies to tighten their internal control policies is likely to cause this shift from informal towards more formal management style within the case company. The reporting relations within the case company are quite clear but lines of reporting upwards are quite complicated. The organisation structure is not very practical in terms of effectively organising work, reporting relations, authorities and responsibilities, and cost control. However, as COSO states, a highly structured organisation may be appropriate for a large entity with numerous operating units and foreign operations, but it may harm a small entity's operations. There seems to be issues with the employees awareness of boundaries of authorisation. This is likely to result from the fact that the responsibilities and authorities of the employees are not effectively and clearly communicated in the case company.

The operational and financial objectives of the case company are clearly defined and effectively communicated. The company's management and employees are committed to these objectives. Further, the situation has changed for the better during the last two years. The company's objectives regarding the compliance with the Sarbanes-Oxley Act S404 are not clearly defined and effectively communicated. In general, the company's management and other employees are not familiar with the S-O act S404 and even the finance staff does not consider having a deep understanding of S404. It seems that the reason for the situation is that there was not sufficient information, support and feedback available for the S-O project team in the implementation process of S404. As the results of this study and the literature review indicate, the most relevant factor of an effective internal control system is the positive attitude of management and other employees toward internal control. The same applies to the S404 requirements and the implementation of the S-O.

It seems that risk management is not an integral part of the management's common work tasks or way of thinking in the case company. However, the Sarbanes-Oxley requirements have caused a more risk-oriented way of thinking within the company's finance by shifting the focus from mere control descriptions toward the company's objectives and risks relating to these objectives. This is because S404 forces companies to evaluate, assess and test the identified business, operational and compliance risks. Additionally, S404 requires process documentation. Preparing process descriptions has led people thinking more about processes than single transactions. This has enabled a more process-oriented mind and people are now able to better evaluate and improve the efficiency of different processes. The process-oriented way of thinking may cause unknown benefits, too. The assessment of risks and processes provides also a better understanding of the company's business and processes. As a result, the S-O act increases control consciousness and knowledge of internal controls. Additionally, as Farrell (2004) notes, this is likely to lead to a greater use of controls, better evaluation of process risks, and more uniform controls throughout the organisation.

The control activities relating to revenue recognition are prioritised in the case company. Also authorities, performance controls, managerial reviews, reconciliations, IT controls and controls relating to the segregation of duties are important in the company. In addition, monitoring of contract terms and conditions and particularly pricing is emphasised in the company. The number of controls relating to operations, financial reporting and information technology has increased during the last two years. Many of the new controls have been put in place when the S-O requirements were implemented in practice in the case company. As a result, the empirical results of the thesis support prior research that the S-O act has increased the number of control activities in the companies that are in the scope. It seems that the case company's management does not pay appropriately attention to control activities. The management's lack of attention toward controls is directly linked to their attitude toward internal control in general. If they do not consider internal control important, they will not pay attention to control activities either. The management's lack of interest may also result from the fact that they do not have appropriate knowledge of the concept of internal control, are not familiar with the company's internal control system or do not understand control activities performed at different levels of the organisation. The empirical results support the claim presented in professional literature that the S-O act requires great efforts from companies. It is worth noticing that S404 sets enormous requirements for companies' control activities that are difficult to perform e.g. in a small reporting unit because of the lack of resources. The S-O act forces companies to invest money and time in additional staff and training of employees, for example. These will have an essential effect on companies' administration costs, including auditing expenses.

COSO emphasises that pertinent information should be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. The quality of information and communication efficiency in the case company is good but not excellent. Usually information is reliable and it is obtainable by appropriate parties. Yet, there seems to be some problems with getting information when it is required. Information is not always the latest available, although it seems that the quality of information has improved during the last two years. In general, the employees of the case company have the means to communicate significant information upstream.

The on-going requirements of the S-O act have been incorporated to the new process of internal control in the case company. As a result, the effect of the act is that the case company conducts an assessment of the effectiveness of its internal controls and tests its key controls. Secondly, these conclusions are incorporated in the corporation's US GAAP financial statements, and are subject to review by the independent auditors. The requirements of S404 have changed considerably the case company's internal audit processes, although these processes have already existed in prior years. The most important change is the shift from a control-oriented toward more risk-oriented way of thinking in the internal control processes.

7.2 MANAGERIAL IMPLICATIONS

The improvement recommendations for the case company are divided into three classes as follows:

1. Factors that enable an effective internal control system
2. Changes to current internal control processes
3. Information and communication related recommendations

The significance of the recommendations is evaluated to be either high, moderate or low.

The first class involves factors that relate to the case company's control environment, including attitudes, ethical values, commitment and competence. Based on the empirical findings of this study, it is recommended that careful attention should be paid on how to commit the entire senior management to internal control. It is essential to change the attitudes of the company's management in a way that they are willing to support and develop the company's internal control system and that they consider internal controls as a way to support the company's business objectives. The significance of this recommendation is evaluated to be high resulting from the fact that it will have a significant effect on the case company's control environment. However, it is reminded that the change for the better commitment to internal control is not likely to happen in a short run but it should be considered as being a long-term target. Additionally, it may well be that the management's high commitment will never be completely achieved. Also it will be challenging to find the means for the change. This recommendation can be generalised to other companies, as well. Particularly companies that have difficulties with the effectiveness of their internal control systems should examine the management's attitudes and the level of commitment to internal controls.

It is also recommended that the case company acknowledges the importance of management's deep understanding of the objectives of possible future implementation processes. For example, based on the results, it is considered that the implementation of the requirements of S404 would have been more effective if the entire management had known the purpose of the act. Understanding, in turn, would have possibly committed the company's management more to the project of the S404. The significance of this recommendation is evaluated to be high. The recommendation regarding an effective implementation will be discussed later.

The second category involves recommendations involving changes to the case company's current internal control processes. It is recommended that the company's management defines and analyses its internal controls and decides the controls that are essential to the achievement of company's objectives. These control activities should be prioritised and the company should focus on improving these controls if there are issues with their effectiveness. All controls should not automatically be considered as important if they are not significant considering the business objectives, for example. Trade-off should be made considering the significance and likelihood of occurrence of the risk because the case company has limited resources. Careful attention should be paid only to the risks that are significant and whose likelihood of occurrence is high. A control should not exist just for itself but it should be put in place to ensure more effective and efficient operations, reliable financial reporting or compliance with laws and regulation. It is recommended that the case company identifies its key controls, which are currently not working effectively. The importance of this recommendation is evaluated to be moderate. To generalise the recommendation, also other companies should examine whether a control is put in place just to comply with S404 or whether the control actually supports business objectives, enables reliable financial reporting and compliance with laws. When companies are trying to achieve the S404 requirements, there may be a danger that the internal control system becomes too heavy and jeopardises effective and efficient operations, for example. Therefore, companies should concentrate on improving their key controls.

It is recommended to ensure that the case company's employees are motivated to perform control activities. Legislation and regulations ensure a minimum standard of conduct. It is worth noticing that people usually perform at a minimum required level as long as it does not cause sanctions or penalties. However, to improve the internal control processes, the case company's management should create incentives to the employees. The majority of people do not perform more than the minimum requirement if there are no incentives in place. As a result, the case company should examine the possibilities of how to support its employees to enable the development of the company's internal control system. Interestingly, the case company's priorities for 2005 include the focus on effective internal controls. However, there are no incentives determined to the employees to meet this goal. The situation is contradictory, because usually if there are no incentives in place, the objective is not considered to be important. Therefore, if the company would like to improve its internal controls, it should create incentives to the employees. The importance of this recommendation is evaluated to be low, if the company's aim is to remain at the same level of effectiveness of its internal control system. However, if the case company aims at more effective internal controls, the significance of the recommendation is high. The recommendations can be generalised to other companies, too.

The third class involves information and communication related recommendations. It is recommended that the case company should pay more attention to communicating about the company's internal control processes and the S-O act within the company. The importance of this recommendation is evaluated to be high, if the company's aim is to commit all employees within the organisation to the effectiveness of the internal control system. Otherwise, the importance is evaluated to be moderate. For example, the implementation of the S-O act would have proceeded more effectively if the requirements had been communicated to the entire senior management and other employees. To generalise, in the beginning of an implementation project it is essential to communicate well the purpose of the project to a management and to ensure that the management is committed to the objectives of the project.

It is important to get people within the organisation to become aware of their concrete tasks and responsibilities in the internal control processes. It is recommended that the concept of internal control is rooted to the people within the organisation. However, it is worth noticing that some individuals, particularly those performing routine tasks, might never become interested in the purpose of internal control activities. In these cases, there should be sufficient monitoring activities in place to ensure the appropriate quality of their work. Additionally, it is recommended that particular attention should be paid to the employees within business activities. This is because they usually operate in a creative environment, in which formal regulation and instructions are not self-evident. It is recommended that internal control processes are presented to people working in business operations by emphasising benefits and introducing the business supportive nature of internal controls. Thus, more attention should be paid to "selling" the requirements of S404 to the case company's leadership team. Therefore, it is recommended that the way of presenting internal controls to the individuals should be selected considering whether the individuals are finance-oriented or not. The significance of these recommendations are evaluated to be moderate.

7.3 DISCUSSION

The research results and conclusions are drawn based on the in-depth analysis of one case customer. The study includes small-scale data, which sets limitations to the generalisation of the findings (Yin 1987, p. 21). The results of the effects of the S-O act S404 on internal control can not be generalised to other companies. However, the study will give some implications on what kind of challenges and benefits companies face when complying the S-O S404. Additionally, the recommendations presented in the managerial implications are to be a great extent generalisable.

The researcher's employment in the case company will affect both the objectivity of the study and the validity of evidence because the researcher has formed a view before the empirical study was conducted. The negative effect on validity is minimized by being aware of this

7

weakness. In addition, data is collected using many sources of evidence and combining data collection methods. (see research material). These are to improve the accuracy of judgements and results. The reliability of the empirical research is increased by using a standard template of the questionnaire and further by structuring the questionnaire well. The empirical research regarding the questionnaire could be replicated by another researcher. However, research data includes also personal notes and direct observation, which affect the results and conclusions. The responses of the twelve questionnaires were manually input to a Excel worksheet that may expose the empirical research to errors. To minimize errors and bias during the research process, manually input data was reviewed three times to check the correctness. Finally, a case study as a research strategy involves ethical issues, such as preserving the case company's anonymity and preserving it from competitors, which influence the research. Because of confidentiality, all information cannot be written in this report. However, a complete picture is captured when presenting the results and conclusions of this study.

This study examines the effects of the S-O act S404 on one case company's internal control practice in Finland and therefore, the research employs a case study approach. The next step would be to examine the results with more extensive research material. For example, it would be interesting to expand data to cover other Finnish companies within the scope, as well. This approach would not enable in-depth analysis but it could examine how other companies see the benefits and problems of S404. It is surprising to notice that one new act enforced in the U.S. is having such an enormous effect throughout the world. It would be interesting to research this global impact of S404 on corporate governance and internal control regulation. Has the new law in the US boosted legislative activities in other countries and if so, how powerful has the effect of this enforcement been? What will be the approach in other countries and, particularly, in the European Union. Examining regulations in different countries would indicate what other countries would prefer: self-regulation or forced legislation in future?

In this thesis the research problem was examined from a management perspective. Additionally, it would be interesting to research the topic from an auditing perspective. How has the act affected auditing practices and what are auditors' views on the act S404?

REFERENCES

Aisbitt, S., Nobes, C. 2001. *"The true and fair view requirement in recent national implementations"*. Accounting and Business Research 2001: Vol. 31, No. 2, p. 83-90.

Alexander, D. 1993. *"A European true and fair view?"*. European Accounting Review 1993: Vol. 2, Issue 1, p.59-80.

Ashton, R.H. 1974. *"An experimental study on Internal Control Judgements"*. Journal of Accounting Research 1974: Vol.12, Issue 1, p. 143-157.

Beasley, M.S, J. V. Carcello, and D. R. Hermanson. 1999. *"Fraudulent Financial Reporting: 1987-1997.* An Analysis of U.S. Public Companies" New York, NY: COSO.

Bryer, R.A. 1993. *"The late nineteenth-century revolution in financial reporting: accounting for the rise of investor or managerial capitalism"*. Accounting, Organizations and Society 1993: Vol. 18, No. 7/8, p. 649-690.

Cadbury Committee. Report of the committee on the Financial Aspects of Corporate Governance, *"The Code of Best Practice"*, 1992. Burgess Science Press.

Canadian Institute of Chartered Accountants (CICA) 1995, *"A Criteria of Control Framework"* (CoCo), quoted in Jackson, P., Livick-Chan, V. 1999. *"Control vs. Controls"*. camagazine.com, October 1999. 15.3.2005.

Canadian Institute of Chartered Accountants (CICA) 1995, *"Guidance on Control"*, Toronto, quoted in Cooper, D. J., Gendron, Y. 2001. *"Power and the criteria of Control"*.

Cohen, J.R., Hanno, D.M. 2000. *"Auditors' Consideration of Corporate Governance and Management Control Philosophy in Preplanning and Planning Judgments."* Auditing: A Journal of Practice and Theory 2000: Vol. 19, Issue 2, p. 133-147.

Cohn, L., Edmondson, G. 2004. "*How Parmalat Went Sour: Here's the skinny on Europe's* *enormous financial scandal*". Business Week. January 1st 2004.

Committee of Sponsoring Organisations of Treadway Committee. *"Internal Control – Integrated framework, Executive Summary"*, 1992.

Cooper, D. J., Gendron, Y. 2001. *"Power and the criteria of Control"*. camagazine.com, March 2001. http://www.camagazine.com/index.cfm?ci_id=6422&la_id=1 15.3.2005.

Critical Control Checklist 2005. Introduction to Completion Instructions – Guidance notes.
Critical Control Checklist 2005. 2. Contract and Order Control.
Critical Control Checklist 2005. 6. Revenue Recognition
Critical Control Checklist 2005. 16. Information Technology
(internal documentation of the case company)

Curtis, M. B., Wu, F. H., 2000. *"The Components of a Comprehensive Framework of Internal Control"* CPA Journal, March 2000.
http://www.nysscpa.org/cpajournal/2000/0300/d64300a.htm 18.8.2005

Drucker, P.F., 1964. Management Controls: New Directions in Basic Research. McGraw-Hill 1964, quoted in Drury 2000.

Drury, C. 2000. Management and Cost Accounting 5th edition. Business Press, Thomson Learning 2000. p. 593-607.

Eisenhardt, K. 1989. "*Building Theories from case study research.*" Academy of Management Review, Vol. 14, pp. 532-550.

European Commission 2003a. Communication from the Commission. *"Reinforcing the Statutory Audit in the EU"*.

European Commission 2003b. Communication from the Commission. "*Modernising Company Law and Enhancing Corporate Governance in the EuropeanUnion - A Plan to*

Move Forward".

European Commission 1998. Communication from the Commission. "*The Statutory Audit in European Union: The Way Forward.*"

European Commission, 1996. "*The Role, Position, and Liability of the Statutory Audit in the European Union: The Way Forward*", quoted in Maijoor, S. 2000.

Ekholm, B-G., Troberg, P. 1996. "*QUO VADIS TRUE AND FAIR VIEW?*". Journal of International Accounting Auditing & Taxation 1998: Vol. 7, Issue 1, p.113-129.

Ekholm, B-G., Troberg, P. 1995. "*Oikeat ja riittävät tiedot – käsite määriteltynä*". Tilintarkastus 1995/5, p.343-346.

Ernst & Young, 2003. Hyvä hallitustapa, p.7.

Evans, L. 2003. "*The true and fair view and the 'fair presentation' override of IAS 1*". Accounting and Business Research 2003: Vol.33, No.4, p.311-325.

Farrell, J. 2004. "*Internal Controls and Managing Enterprise-Wide Risks*". CPA Journal 2004: Vol. 74, Issue 8, p. 11-12.

Foreign Corrupt Practices Act of 1977. Legislative History. Senate Report No. 95-114. Integrity of Accounting Records and Reports.
www.usdoj.gov/criminal/fraud/fcpa/1977sen.htm 23.2.2005

Gordon, D. M. 1994. "*Bosses of different stripes: A cross-national perspective on monitoring and supervision.*" American Economic Review 1994: Vol. 84, Issue 2, p. 375-379.

HEX Plc, the Central Chamber of Commerce of Finland, the Confederation of Finnish Industry and Employers, 2003. Corporate Governance Recommendation for Listed Companies.

Hermanson, H.M. 2000. *"An analysis of the demand for reporting on internal control"*. Accounting Horizons 2000: Vol. 14, No. 3, pp. 325-341.

Hirvonen, A., Niskakangas, H., Steiner, M-L. Corporate Governance – Hyvä omistajaohjaus ja hallitustyöskentely 2003, p.21, WSOY, Helsinki.

Horngren, C.T., Sundem, G.L., 1993. Introduction of Management Accounting 9th Edition. Prentice-Hall International. p. 295-304.

International Accounting Standards Board (IASB) 2003, IFRS-standardit 2003, Jyväskylä.

ICMP Validation Summary 2004. (internal documentation of the case company)

Jackson, P., Livick-Chan, V. 1999. *"Control vs. Controls"*. camagazine.com, October 1999. http://www.camagazine.com/index.cfm/ci_id/5914/la_id/1.htm 15.3.2005.

Business Ethics 2005. (internal documentation of the case company)

Maijoor, S. 2000. *"The Internal Control Explosion"*. International Journal of Auditing, Vol. 4, p. 101-109.

McNally, J. S. 2004. "T*he Year of Internal Control: The Clock Is Ticking for Sarbanes-Oxley Compliance."* Pennsylvania CPA Journal, Spring 2004, Vol. 75, Issue 1, p. 1-5.

McNamee, P. 1993. *"The new yellow book: Focus on internal controls."* Journal of Accountancy, 1993, Vol. 176, Issue 4, p. 83-86.

McMullen, D.A., Raghunandan, K., Rama, D.V. 1996. *"Internal Control Reports and Financial Reporting Problems"*. Accounting Horizons 1996: Vol. 10, No. 4, pp. 67-75.

Merchant, K. 1998. *Modern Management Control Systems*, New Jersey, Prentice Hall, quoted in Maijoor 2000 and in Drury 2000.

Mäkinen, L. 1996. *"Väärä ja puutteellinen kuva"*. Tilintarkastus 1996/1

Määttä, S. 2000. *"TRUE AND FAIR VIEW – Ajatuksia oikeista ja riittävistä tiedoista ja kuvasta erityisesti Suomessa käydyn keskustelun valossa"*. Series Discussion and Working Papers 2:2000. Kirjapaino Grafia Oy, Turku.

National Commission on Fraudulent Financial Reporting. 1987. Report of the National Commission on Fraudulent Financial Reporting, New York. (www.coso.org/NCFFR.pdf 20.2.2005)

OECD Principles of Corporate Governance 1999.

OPMAC minutes of meetings Q1-Q4'2004 and Q1'2005. (internal documentation of the case company)

Ouchi, W. G. 1979. A conceptual framework for the design of organizational control mechanism, Management Science, p. 833-848, quoted in Drury 2000.

Parker R. H., Nobes, C. W. 1991. *"'True and Fair'; UK Auditor's View"*. Accounting and Business Research 1991: Vol. 21, Issue 84, p. 349-361.

Policy Deployment Nordic 2005. (internal documentation of the case company)

Power, M. 1997. *The Audit Society: Rituals of Verification.* Oxford University Press, quoted in Maijoor, S. 2000. *"The Internal Control Explosion"*. International Journal of Auditing, Vol. 4, p. 101-109.

Quall, J. C. 2004. *"Implementing Section 404: A Practical Approach to the Sarbanes-Oxley Act"*. Cpa Journal New York: Aug 2004, Vol. 74, Issue 8, p. 52-58.

Raghunandan, K., Rama, D.V. 1994. *Management Reports after COSO*. Internal Auditor, August 1994, p. 54-59.

Riistama, V. 1996. *"Oikeat ja riittävät tiedot meno-tulo –teorian näkökulmasta"*. Tilintarkastus 1996/1, p. 7-10.

Sarbanes-Oxley documentation of the case company: Revenue and Receivables Cycle. Accounting Cycle.

SAS No. 55 "Consideration of Internal Control in a Financial Statement Audit", American Institute of Certified Public Accountants, quoted in McNamee, P. 1993. "The new yellow book: Focus on internal controls." Journal of Accountancy, 1993, Vol. 176, Issue 4, p. 83-86.

Scapens, R. 1990. *"Researching management accounting practise: The role of case study methods."* British Accounting Review 1990: Vol. 22, p. 259-281.

Securities and Exchange Commission. SEC Final Rules, Release No. 33-8545, 2.3.2005. Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports of Non-Accelerated Filers and Foreign Private Issuers; Extension of compliance dates. http://www.sec.gov/rules/final.shtm

Securities and Exchange Commission. SEC Final Rules, Release No. 33-8392, 24.2.2004. Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports. http://www.sec.gov/rules/final.shtml

Securities and Exchange Commission. SEC Final Rules, Release No. 33-8238, 5.6.2003. Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports. http://www.sec.gov/rules/final.shtml

Select Committee of the House of Lords on the Companies Bill 1896. Proceedings of the Committee, Minutes of Evidence, quoted in Bryer, R.A. 1993. "*The late nineteenth-century revolution in financial reporting: Accounting for the rise of investor or managerial capitalism*". Accounting, Organizations and Society 1993: Vol. 18, No. 7/8, p. 649-690.

Spira, L.F., Page, M. 2003. *"Risk management: The reinvention of internal control and the* *changing role of internal audit."* Accounting, Auditing and Accountability Journal 2003: Vol. 16, No. 4, pp. 640-661.

Society of Management Accountants of Canada. *"Corporate Governance: The Role of Internal Control"*. (www.aicpa.org/cefm/management_control_04.asp 21.2.2005)

Tilintarkastusalan suositukset 2003, KHT-Media, Jyväskylä 2003.

Van Hulle, K. 1993. *"Truth and untruth about true and fair: a commentary on 'A European true and fair view' comment"*. The European Accounting Review 1993: Vol. 2, Issue 1, p. 99-104.

Wallace, W. A. 1982. *"Should CPAs' reports on internal control be required? Survey evidence on the effects of such a requirement."* Akron Business & Economics Review 13, Spring, pp. 20-23, quoted in Hermanson, H.M. 2000. "An analysis of the demand for reporting on internal control". Accounting Horizons 2000: Vol. 14, No. 3, pp. 325-341.

Widener, S.K., Selto, E.H. 1998. *"Management Control Systems and Boundaries of the Firm: Why do Firms Outsource Internal Auditing Activities?"* Journal of Management Accounting Research 1999: Vol. 11, p. 45-74.

Williams, D.W. 1985. *"Legal perspectives on auditing"* in D. Kent, M. Sherer, S. Turley (eds). Current Issues in Auditing, Harper and Row, London, quoted in Parker and Nobes, 1991. *"'True and Fair'; UK Auditor's View"*. Accounting and Business Research 1991: Vol. 21, Issue 84, p. 349-361.

Yin, R. 1987. "*Case study research. Design and methods."* Volume 5, Newbury Park, Sage.

www.asb.org.uk
www.coso.org/publications
www.fasb.org
www.nasdaq.com/about/LegalCompliance.stm

www.nyse.com/regulation

www.sec.gov

www.sox-online.com

APPENDIXES

APPENDIX 1: THE TABLE OF CONTENT – THE SARBANES-OXLEY ACT OF 2002

TITLE I—PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
Sec. 101. Establishment; administrative provisions.
Sec. 102. Registration with the Board.
Sec. 103. Auditing, quality control, and independence standards and rules.
Sec. 104. Inspections of registered public accounting firms.
Sec. 105. Investigations and disciplinary proceedings.
Sec. 106. Foreign public accounting firms.
Sec. 107. Commission oversight of the Board.
Sec. 108. Accounting standards.
Sec. 109. Funding
.

TITLE II—AUDITOR INDEPENDENCE
Sec. 201. Services outside the scope of practice of auditors.
Sec. 202. Preapproval requirements.
Sec. 203. Audit partner rotation.
Sec. 204. Auditor reports to audit committees.
Sec. 205. Conforming amendments.
Sec. 206. Conflicts of interest.
Sec. 207. Study of mandatory rotation of registered public accounting firms.
Sec. 208. Commission authority.
Sec. 209. Considerations by appropriate State regulatory authorities.

TITLE III—CORPORATE RESPONSIBILITY
Sec. 301. Public company audit committees.
Sec. 302. Corporate responsibility for financial reports.
Sec. 303. Improper influence on conduct of audits.
Sec. 304. Forfeiture of certain bonuses and profits.
Sec. 305. Officer and director bars and penalties.
Sec. 306. Insider trades during pension fund blackout periods.
Sec. 307. Rules of professional responsibility for attorneys.
Sec. 308. Fair funds for investors.

TITLE IV—ENHANCED FINANCIAL DISCLOSURES
Sec. 401. Disclosures in periodic reports.
Sec. 402. Enhanced conflict of interest provisions.
Sec. 403. Disclosures of transactions involving management and principal stockholders.
Sec. 404. Management assessment of internal controls.
Sec. 405. Exemption.
Sec. 406. Code of ethics for senior financial officers.
Sec. 407. Disclosure of audit committee financial expert.
Sec. 408. Enhanced review of periodic disclosures by issuers.
Sec. 409. Real time issuer disclosures.

TITLE V—ANALYST CONFLICTS OF INTEREST
Sec. 501. Treatment of securities analysts by registered securities associations and national securities exchanges.

TITLE VI—COMMISSION RESOURCES AND AUTHORITY
Sec. 601. Authorization of appropriations.
Sec. 602. Appearance and practice before the Commission.
Sec. 603. Federal court authority to impose penny stock bars.

Sec. 604. Qualifications of associated persons of brokers and dealers.

TITLE VII—STUDIES AND REPORTS
Sec. 701. GAO study and report regarding consolidation of public accounting firms.
Sec. 702. Commission study and report regarding credit rating agencies.
Sec. 703. Study and report on violators and violations
Sec. 704. Study of enforcement actions.
Sec. 705. Study of investment banks.

TITLE VIII—CORPORATE AND CRIMINAL FRAUD ACCOUNTABILITY
Sec. 801. Short title.
Sec. 802. Criminal penalties for altering documents.
Sec. 803. Debts nondischargeable if incurred in violation of securities fraud laws.
Sec. 804. Statute of limitations for securities fraud.
Sec. 805. Review of Federal Sentencing Guidelines for obstruction of justice and extensive criminal fraud.
Sec. 806. Protection for employees of publicly traded companies who provide evidence of fraud.
Sec. 807. Criminal penalties for defrauding shareholders of publicly traded companies.

TITLE IX—WHITE-COLLAR CRIME PENALTY ENHANCEMENTS
Sec. 901. Short title.
Sec. 902. Attempts and conspiracies to commit criminal fraud offenses.
Sec. 903. Criminal penalties for mail and wire fraud.
Sec. 904. Criminal penalties for violations of the Employee Retirement Income Security Act of 1974.
Sec. 905. Amendment to sentencing guidelines relating to certain white-collar offenses.
Sec. 906. Corporate responsibility for financial reports.

TITLE X—CORPORATE TAX RETURNS
Sec. 1001. Sense of the Senate regarding the signing of corporate tax returns by chief executive officers.

TITLE XI—CORPORATE FRAUD AND ACCOUNTABILITY
Sec. 1101. Short title.
Sec. 1102. Tampering with a record or otherwise impeding an official proceeding.
Sec. 1103. Temporary freeze authority for the Securities and Exchange Commission.
Sec. 1104. Amendment to the Federal Sentencing Guidelines.
Sec. 1105. Authority of the Commission to prohibit persons from serving as officers or directors.
Sec. 1106. Increased criminal penalties under Securities Exchange Act of 1934.
Sec. 1107. Retaliation against informants.

APPENDIX 2: ACCOUNTING CYCLE

ACC.001	FIXED EXPENSES / COSTS ACCRUALS
ACC.002, .004	RENTAL & FSMA ACCRUALS AND DEFERRALS
ACC.003	LEASE ACCOUNTING
ACC.005	BILLING WITH CAPITAL – billing & accounts payable
ACC.006	REVENUE & COST ELIMINATION
ACC.007	INVENTORY PROVISIONS
ACC.008	INTERCOMPANY
ACC.009	INCOME TAX & VAT
ACC.010	DEPRECIATIONS FOR FIXED ASSETS
ACC.011	BAD DEBT PROVISION
ACC.012	ORS REVENUE AND COST ACCRUAL
ACC.013	RESTRUCTING PROVISION
ACC.014	SOLD TONER TO the other subsidiary
ACC.015	PAYROLL / XSAP INTERFACE
ACC.017	CONSUMABLES AT CUSTOMERS
ACC.018	TRANSFER to the other subsidiary - FIXED EXPENSES & BALANCE SHEET
ACC.019	JOURNAL RAISING PROCESS
ACC.020	REVIEW PROCESS
ACC.021	SUBMIT TO REPORTS TO HQ
ACC.022	BALANCE SHEET RECONCILIATIONS - local & inter-company
ACC.023	ORS CUT-OFF TESTING
ACC.024	JOURNAL AUTHORISATION CHECK

APPENDIX 3: REVENUE AND RECEIVABLES CYCLE

REV.001	PRE ORDER
REV.002.1	ORDER / CONTRACT VALIDATION
REV.002.2	CONTRACT TERMINATION
REV.003	CREATE / VALIDATE CUSTOMER
REV.004	CREDIT ASSESSMENT
REV.005.1	CREATE ORDER / CONTRACT
REV.005.2	CREATE SERVICE ORDER
REV.005.3	CREATE JOB TICKET ORDER
REV.005.4	CREATE CONSUMABLES ORDER
REV.006	DELIVER / COLLECT ORDER
REV.007	INVOICE CUSTOMER ORDER
REV.008.1	CUSTOMER CONTRACT INITIATION
REV.008.2	REPETITIVE CONTRACT BILLING
REV.008.3	CANCEL & REISSUE INVOICE / CREATE CREDIT NOTE
REV.008.4	CONTRACT PRICE INCREASE
REV.010.1	CASH ALLOCATION
REV.010.2	SAP DUNNING
REV.010.3	COLLECTION PROCESS
REV.010.4	UN-MATCHED CREDITS ADMINISTRATION
REV.010.5	LEGAL COLLECTIONS
REV.010.6	WRITE-OFF PROCESS
REV.010.7	INTEREST CHARGE ADMINISTRATION

APPENDIX 4: COVERING LETTER AND THE QUESTIONNAIRE

Covering letter

Dear Recipient,

I am preparing my Master's thesis at Helsinki School of Economics. The objective of my study is to depict the effect of the Sarbanes-Oxley Act S404 to Internal Control Practice. Please find attached a questionnaire, which is an essential part of this study. The questions are related to the internal control system of the case company. The instructor of the study is professor Pontus Troberg.

The Sarbanes-Oxley Act came into effect in the United States on July 30th, 2002. The Act applies to the companies whose shares are listed in a securities exchange registered with the SEC. The objective is to strengthen corporate governance and restore trust in the public securities market. **Section 404** specifies the requirements set to the management's report on internal control over financial reporting.

This questionnaire is based on the COSO Framework in which internal control of a company consists of the following components:

1. Control Environment
2. Risk assessment
3. Control Activities
4. Information and Communication
5. Monitoring

The questionnaire has six parts that include both multiple choice and open questions. Please note that the focus of this questionnaire is the company Y FINLAND. I would appreciate if you filled out the questionnaire and returned it back by the 24th of May. Filling out the questionnaire takes about 20 – 30 minutes.

All information will be handled confidentially and no names or positions will be mentioned when the results are presented in the study.

Thank you very much for your participation!

Best regards,

Reetta Liikala
Helsinki School of Economics
+358 50 359 9714
reetta.liikala@kyyppari.hkkk.fi

Part 1: Background information

Respondent's background information

1. Respondent's name ____________________
2. Respondent's position ____________________
3. Respondent's function or unit ____________________

4. I participate in the Sarbanes-Oxley project in Finland

☐ Yes

☐ No

5. I participate in the ICMP Process / Internal Audit in Finland

☐ Yes

☐ No

Part 2: Control Environment

6. Please rank your answer with a cross in the table below.

Please also mark in the last column " +/- ":

Mark + if you regard that the factor has improved during the last 1-2 years, or mark - if you think that the change in the factor has been unfavourable. If the cell is coloured with black, there is no need for comparison.

1 = Strongly agree

3 = Neither agree nor disagree

5 = Strongly disagree

CNS = Can Not Say

+ = Change for the better

- = Change for the worse

Strongly agree — *Neither agree nor disagree* — *Strongly disagree*

Factor	1	2	3	4	5	*CNS*	+/-
Honesty, Integrity and Ethical Values							
Behaviour of the staff is very ethical.							
The employees are honest and reliable.							

Factor	*1*	*2*	*3*	*4*	*5*	*CNS*	*+ / -*
The code of conduct is followed in *actual* behaviour.							
The company's ethical values are clearly communicated.							
Staff has been clearly communicated what is right and what is wrong.							
Top management is showing by their example ethically high behaviour to other employees.							
Incentives							
Management encourages the staff to good performance.							
As a superior, you encourage your team to the achievement of objectives.							
Making profits in the short run is emphasized as a company's objective.							
Increase of revenue is highlighted as a company's objective.							
Top and operational management are constantly aware of activities of their staff.							
Internal control processes properly ensure that behaviour out of place is detected and reported.							
Top management pays clear attention to incentives.							
Commitment to Competence							
Competence requirements are defined to different job assignments.							
Individuals have sufficient skills to perform their work.							
The Board of Directors and Audit Committee (OPMAC)							
The board of directors and OPMAC are setting "tone at the top" and influence significantly the control environment.							
OPMAC is active and has an important role in assuring effective internal control.							
OPMAC and top management discuss together the company's plans, performance and problems in these.							
Assigning Authority and Responsibility							
Authority and responsibility is significantly cascaded to different levels within the company.							
Reporting relations and authorities have been clearly written down.							
Reporting relations and authorities have been clearly communicated within the company.							
The employees are aware of the boundaries of authorities.							
The employees are encouraged to solve problems independently.							
The staff is aware of procedures (which describe and define how a specific work is carried out properly).							
The scope of authority of employees is appropriate.							
As a superior, you delegate appropriately responsibility and authority to your team members.							
Management Philosophy and Operating Style							
Top management is honest and reliable.							
Top management has taken a positive stand and is interested in effective internal control.							
Top management acts as an example and shows that effective internal control is important.							

Factor	*1*	2	*3*	*4*	*5*	*CNS*	+ / -
The company is directed informally.							
The company is directed formally (written procedures, performance measures, exception reporting etc.)							
Financial difficulties and the company history have affected the management style.							

7. Has the management style changed towards formal or informal during the last 1-2 years? Please mark your answer below.

☐ It is more formal than earlier.

☐ It is more informal than earlier.

1 = Strongly agree

3 = Neither agree nor disagree

5 = Strongly disagree

CNS = Can Not Say

+ = Change for the better

- = Change for the worse

Strongly agree *Neither agree nor disagree* *Strongly disagree*

Factor	*1*	2	*3*	*4*	*5*	*CNS*	+ / -
Organisation structure							
Reporting relations within the company functions are clear.							
Reporting relations from the company upwards are clear.							
Organisation structure is practical and supports the achievement of objectives.							
Staff Procedures and Practices							
The staff is committed to the operational and financial objectives of the company.							
The staff is committed to the legislative objectives of the company.							
The staff is encouraged to educate and develop themselves.							
Non-compliance with the code of conduct is not accepted.							
The company tries to commit the staff to the company by e.g. job rotation, incentives and rehabilitation programs.							
Competence is highlighted in recruiting.							

8. If you disagreed with some of the factors regarding "Organization structure", please explain shortly why.

____

____

9. In your opinion, who is responsible for internal control?

10. How would you describe shortly your role in organising internal control? Has your role changed during the last two years? Why?

11. How important do you consider internal control as a part of company's operations?

Part 3: Risk assessment

Every company is faced with both external and internal risks that can relate to the company (competition, customer needs and expectations, development of technology) or to a company's operations such as communication breakdown, the quality of staff, and changes in operations. In addition, changes in the financial and legislative environment, technology or competition are a part of risk assessment. ***Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how risks should be managed"(COSO).***

12. Please rank your answer with a cross in the table below.

Please also mark in the last column " +/- ":

Mark + if you regard that the factor has improved during the last 1-2 years, or

mark - if you think that the change in the factor has been unfavourable.

If the cell is coloured with black, there is no need for comparison.

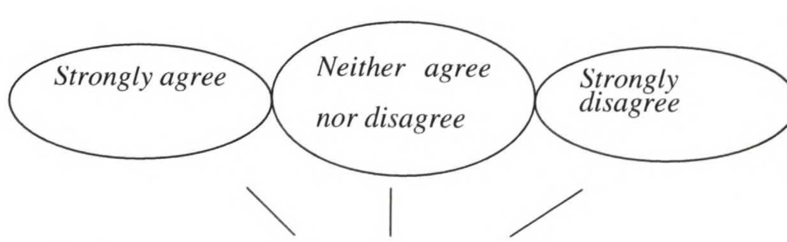
1 = Strongly agree

3 = Neither agree nor disagree

5 = Strongly disagree

CNS = Can Not Say

+ = Change for the better



- = Change for the worse

Factor	*1*	2	*3*	*4*	*5*	*CNS*	+ / -
The Objectives of the Company							
The operational objectives of the company are defined clearly and communicated to the staff.							
The objectives regarding the compliance of laws and regulation are defined clearly and communicated to the staff.							
Factor	***1***	*2*	*3*	*4*	*5*	*CNS*	+ / -
Top management invests time in defining objectives and communicating these objectives to the staff.							
The company's objectives regarding the compliance with Sarbanes-Oxley Act are defined and communicated clearly.							
Risks and Risk analysis							
Management invests time in identifying and analyzing organisational risks and takes actions in order to manage those risks.							
Identifying and analyzing risks is more and more important in my work today.							
Methods for risk assessment offered by the company are good.							
Risk management is extensive in the company (e.g. contracts, pricing, and insurances as means).							

Part 4: Control Activities

Control activities are policies and procedures which help ensure that management directives are carried out in the organisation. The control activities occur at all levels and in all functions of the organisation and they can be e.g. preventative, detective, manual or IT. They can also be operational, financial or regulative such as the segregation of duties, physical controls, reviews of operating performance etc.

13. Please rank your answer with a cross in the table below.

Please also mark in the last column " +/- ":

Mark + if you regard that the factor has improved during the last 1-2 years, or

mark - if you think that the change in the factor has been unfavourable.

If the cell is coloured with black, there is no need for comparison.

1 = Strongly agree

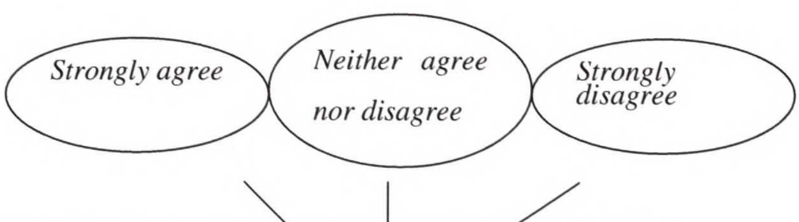
3 = Neither agree nor disagree

5 = Strongly disagree

CNS = Can Not Say

+ = Change for the better

- = Change for the worse



Factor	*1*	2	*3*	*4*	*5*	*CNS*	+ / -

Control Activities							
Top management pays a lot of attention to control activities.							
The segregation of duties is sufficient so that errors and improper behaviour can be avoided.							
Factor	*1*	2	*3*	*4*	*5*	*CNS*	+ / -
Management determines necessary control activities in a risk assessment.							

14. In your opinion, has the number of control activities relating to operations increased during the last 1-2 years?

☐ Yes

☐ No

15. In your opinion, has the number of control activities relating to the financial reporting increased during the last 1-2 years?

☐ Yes

☐ No

16. In your opinion, has the number of IT control activities relating to operations and the financial reporting increased during the last 1-2 years?

☐ Yes

☐ No

17. Please describe control activities you consider the most significant in your function?

___

___

___

Part 5: Information and Communication

Information is needed in every level of organisation so that business can be managed and controlled. Information is utilised in making operational decisions, monitoring activities, and preparing financial reports. The following multiple choice questions cover the quality of information and the efficiency of communication.

18. Please rank your answer with a cross in the table below.

Please also mark in the last column " +/- ":

Mark + if you regard that the factor has improved during the last 1-2 years, or

mark - if you think that the change in the factor has been unfavourable.

If the cell is coloured with black, there is no need for comparison.

1 = Strongly agree

3 = Neither agree nor disagree

5 = Strongly disagree

CNS = Can Not Say

+ = Change for the better

- = Change for the worse

Strongly agree *Neither agree nor disagree* *Strongly disagree*

Factor	*1*	2	*3*	*4*	*5*	*CNS*	+ / -
The Quality of Information							
Information is appropriate; you are getting all necessary information that is relevant for you to do your work well.							
You are getting information timely.							
Information is valid; you always get the latest information.							
Information is right and reliable.							
Information is open; it is accessible to all entitled parties.							
The quality has improved during the last two years.							
Communication							
Communication is efficient within the whole company flowing down, across and up the organisation.							
Top management has given a clear message to the staff that control responsibilities have to be taken seriously.							
The employees know their own work task and responsibility in the internal control system.							
The employees know how an individual work task relates to work of others.							
The employees have means of communicating significant information upstream.							
The superiors have a clear interest to listen the employees and they want to know about problems.							
Communication towards customers and suppliers is efficient (e.g. customer complaints, customer credit information and other background information).							

Part 6: Sarbanes-Oxley

If you take part in the Sarbanes-Oxley project in Finland, please answer the questions below.

19. In your opinion, what are the benefits that the compliance with Sarbanes-Oxley Act has brought in ensuring a true and fair view in the financial reporting?

20. Please describe problems and challenges that relate to the compliance with Sarbanes-Oxley Act

THANK YOU FOR YOUR ANSWERS!